

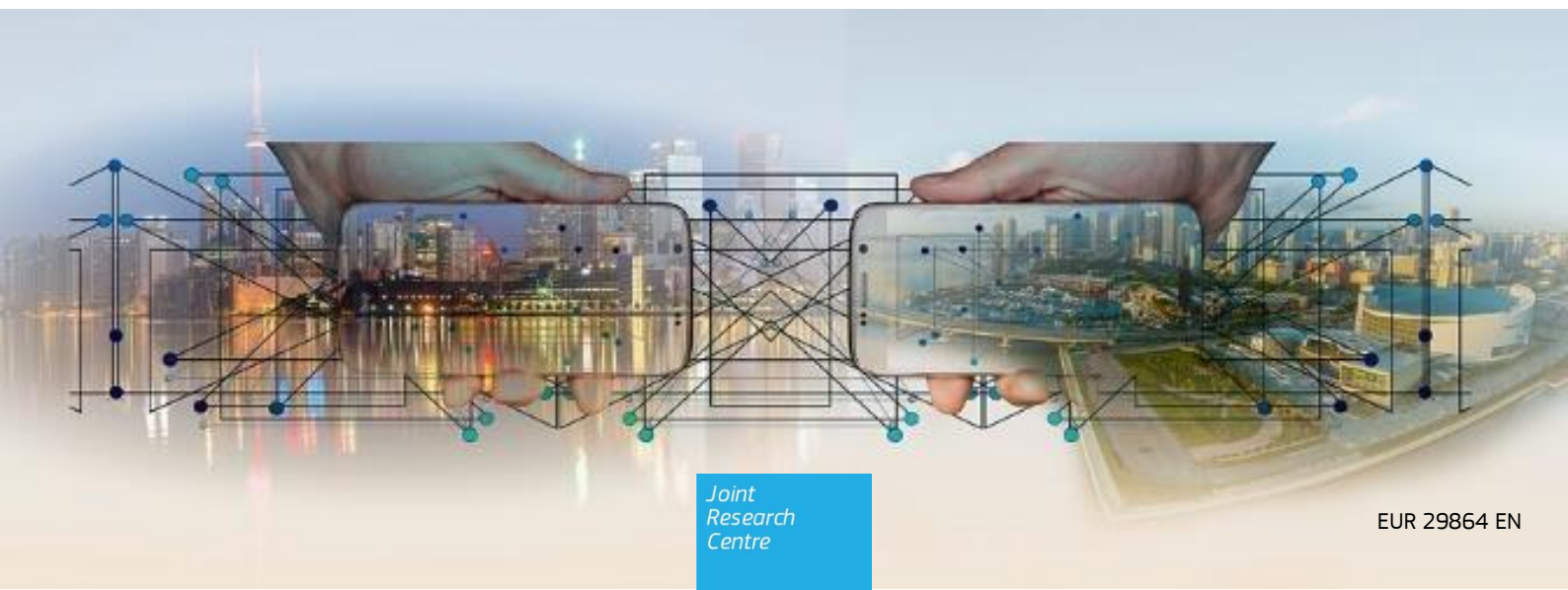
JRC SCIENCE FOR POLICY REPORT

Security and Defence Research in the European Union: A landscape review

*With a specific focus on
man-made risks and threats
intended to cause harm*

Editors: G. Bordin, M. Hristova, E. Luque-Perez

2019



This publication is a Science for Policy report by the Joint Research Centre (JRC), the European Commission's science and knowledge service. It aims to provide evidence-based scientific support to the European policymaking process. The scientific output expressed does not imply a policy position of the European Commission. Neither the European Commission nor any person acting on behalf of the Commission is responsible for the use that might be made of this publication. For information on the methodology and quality underlying the data used in this publication for which the source is neither Eurostat nor other Commission services, users should contact the referenced source. The designations employed and the presentation of material on the maps do not imply the expression of any opinion whatsoever on the part of the European Union concerning the legal status of any country, territory, city or area or of its authorities, or concerning the delimitation of its frontiers or boundaries.

Contact information

Name: Guy Bordin, Mayya Hristova and Encarnacion Luque-Perez

Address: Rue du Champ de Mars 21, 1049 Brussels, Belgium

Email: Guy.BORDIN@ec.europa.eu; Mayya-Anatolieva.HRISTOVA@ec.europa.eu; Encarnacion.LUQUE-PEREZ@ec.europa.eu

Tel.: +32 22987971; +32 22956998; +32 22966698

EU Science Hub

<https://ec.europa.eu/jrc>

JRC117742

EUR 29864 EN

PDF

ISBN 978-92-76-11442-0

ISSN 1831-9424

doi:10.2760/100724

Luxembourg: Publications Office of the European Union, 2019

© European Union, 2019



The reuse policy of the European Commission is implemented by the Commission Decision 2011/833/EU of 12 December 2011 on the reuse of Commission documents (OJ L 330, 14.12.2011, p. 39). Except otherwise noted, the reuse of this document is authorised under the Creative Commons Attribution 4.0 International (CC BY 4.0) licence (<https://creativecommons.org/licenses/by/4.0/>). This means that reuse is allowed provided appropriate credit is given and any changes are indicated. For any use or reproduction of photos or other material that is not owned by the EU, permission must be sought directly from the copyright holders.

All content © European Union, 2019, except: Cover page, source: pixabay.com

How to cite this report: Bordin, G., Hristova, M., Luque-Perez, E. (eds.), *Security and Defence Research in the European Union: A landscape review*, EUR 29864 EN, Publications Office of the European Union, Luxembourg, 2019, ISBN 978-92-76-11442-0, doi:10.2760/100724, JRC117742.

Contents

Abstract.....	1
Acknowledgements	2
Executive summary.....	3
1 Introduction.....	4
2 The security and defence situation in the European Union.....	6
2.1 Border control.....	6
2.1.1 What is border control?	6
2.1.2 A political priority of the European Commission.....	7
2.1.3 The possible evolution of border control within the next 5 to 10 years.....	8
2.1.4 Stakeholders.....	8
2.1.5 Legislation and reference documents.....	11
2.2 Critical infrastructure protection.....	12
2.2.1 What is a critical infrastructure?	12
2.2.2 Threats to critical infrastructures.....	13
2.2.3 The European Union scene and beyond	14
2.2.4 Possible evolution within the next 5 years.....	15
2.2.5 Stakeholders.....	16
2.2.6 Legislation and reference documents.....	19
2.3 Public spaces protection.....	20
2.3.1 What are soft targets / public spaces?	20
2.3.2 Protecting public spaces.....	21
2.3.3 The European Union scene and beyond	21
2.3.4 Possible evolution within the next 5 years.....	23
2.3.5 Stakeholders.....	24
2.3.6 Legislation and reference documents.....	26
2.4 Critical supplies security.....	26
2.4.1 What are critical supplies?.....	26
2.4.2 Securing the supply of raw materials and fuels in the European Union	27
2.4.3 Possible evolution within the next 5 years.....	31
2.4.4 Stakeholders.....	31
2.4.5 Legislation and reference documents.....	33
2.5 Cybersecurity.....	34
2.5.1 What are cyber-threats?.....	34
2.5.2 How do 'state hackers' or 'hacktivists' operate?.....	35
2.5.3 Reform of cybersecurity in the European Union	35
2.5.4 Possible evolution within the next 5 years.....	39
2.5.5 Stakeholders.....	39

2.5.6	Legislation and reference documents.....	43
2.6	Chemical, biological, radiological, nuclear and high-yield explosive threats	44
2.6.1	What are chemical, biological, radiological, nuclear and high-yield explosive hazardous materials?.....	44
2.6.2	The European Union scene.....	45
2.6.3	International agreements.....	46
2.6.4	Possible evolution within the next 5 years.....	47
2.6.5	Stakeholders.....	48
2.6.6	Legislation and reference documents.....	53
2.7	Hybrid threats.....	54
2.7.1	What are hybrid threats?.....	54
2.7.2	How do hybrid attackers operate?.....	54
2.7.3	Countering hybrid threats in the European Union	56
2.7.4	Possible evolution of hybrid threats within the next 5 years.....	56
2.7.5	Stakeholders.....	57
2.7.6	Legislation and reference documents.....	60
2.8	Combating radicalisation to terrorism.....	61
2.8.1	The European Union's rationale for focusing on eradicating terrorism at its source — the why and what	61
2.8.2	How do terrorists recruit and operate?.....	61
2.8.3	The European Union's strategy for combating radicalisation and recruitment to terrorism.....	63
2.8.4	Possible evolution of radicalisation within the next 5 years.....	65
2.8.5	Stakeholders.....	65
2.8.6	Legislation and reference documents.....	67
2.9	Fighting against terrorism financing.....	68
2.9.1	The European Union's rationale for focusing on combating terrorism financing — the why and the what.....	68
2.9.2	How does terrorism financing work?	69
2.9.3	Countering terrorism financing in the European Union	71
2.9.4	Possible evolution of terrorism financing within the next 5 years.....	73
2.9.5	Stakeholders.....	74
2.9.6	Legislation and reference documents.....	76
2.10	Space.....	78
2.10.1	The importance of space for the European Union and for security	78
2.10.2	The European Union's role and ambition in space	79
2.10.3	The international scene.....	81
2.10.4	Possible evolution of space within the next 5 to 10 years.....	82
2.10.5	Stakeholders.....	86
2.10.6	Legislation and reference documents.....	90
2.11	Defence.....	93

2.11.1	The European Security Strategy (2003).....	93
2.11.2	The European Union internal security strategy (2010)	94
2.11.3	The European agenda on security (2015).....	95
2.11.4	The European Union global strategy (2016).....	95
3	Security and defence research	96
3.1	History and evolution of European Union security research.....	96
3.1.1	First steps: the Group of Personalities and the preparatory action on security research.....	96
3.1.2	European Security Research Advisory Board (2005-2006) and the seventh research framework programme.....	97
3.1.3	The European Security Research and Innovation Forum	100
3.1.4	Other funding programmes related to security (2007-2013).....	101
3.1.5	Horizon 2020 (2014-2020).....	103
3.1.6	Other funds related to security (2014-2020).....	107
3.1.7	Security advisory groups after the European Security Research and Innovation Forum.....	109
3.1.8	Horizon Europe (2021-2027).....	110
3.2	History and evolution of European Union defence research	114
3.2.1	European Defence Agency — first research activities outside the European Union budget	114
3.2.2	The Commission communication of July 2013.....	114
3.2.3	The European defence action plan (2016)	115
3.2.4	First steps in European Union-funded defence research: the pilot project (2015-2016).....	115
3.2.5	The Group of Personalities (2015-2016).....	116
3.2.6	The preparatory action on defence research (PADR) (2017-2019)	116
3.2.7	The future of European defence research: the European Defence Fund	118
3.2.8	The European defence research programme and Horizon Europe.....	120
3.2.9	Other funds related to defence (2014-2020).....	120
3.3	Analysis of Horizon 2020 security- and defence-related research projects.....	127
3.3.1	Methodological introduction	127
3.3.2	Analysis of results.....	128
3.4	JRC security-related research.....	142
3.4.1	Border control.....	142
3.4.2	Critical infrastructure protection.....	144
3.4.3	Public space protection.....	145
3.4.4	Critical supplies security.....	146
3.4.5	Cybersecurity.....	147
3.4.6	Chemical, biological, radiological, nuclear and high-yield explosive threats	149
3.4.7	Hybrid threats.....	150
3.4.8	Space.....	151
4	Future avenues for security and defence research and development	153
4.1	Subject-specific developments	153
4.1.1	Border control.....	153

4.1.2	Critical infrastructure protection	153
4.1.3	Public space protection.....	154
4.1.4	Critical supplies security	155
4.1.5	Cybersecurity.....	155
4.1.6	Chemical, biological, radiological, nuclear and high-yield explosive threats	156
4.1.7	Hybrid threats.....	156
4.1.8	Combating radicalisation.....	157
4.1.9	Fighting against terrorism financing	157
4.1.10	Space.....	157
4.2	Horizon scanning on security	158
4.2.1	Methodology	158
4.2.2	Results	158
4.2.3	Comments	166
5	Conclusions.....	167
	Bibliography.....	168
	References	168
	Legislation and policy documents from the European Union institutions.....	174
	Abbreviations	183
	List of figures	191
	List of tables.....	193
	Annexes	195
	Annex 1. List of European critical infrastructure sectors as listed in Directive 2008/114/EC	195
	Annex 2. Examples of critical infrastructure disruptions	195
	Annex 3. Permanent structured cooperation projects.....	197
	Annex 4. Horizon 2020 security- and defence-related projects (master table).....	198
	Annex 5. Data from the analysis of Horizon 2020 security- and defence-related projects	222
	Annex 6. Entities participating in H2020 security- and defence-related projects.....	251
	Annex 7. Horizon scanning on security: selected items which inspired collective clusters	259

Abstract

This landscape report describes the state of play of the European Union's policies and activities in security and defence and the EU-funded research aimed at supporting them, with an exclusive focus on intentional harm. It is organised around several thematic building blocks under the umbrella of the three core priorities defined in the European agenda on security.

The report reviews the current main risks and threats but also those that may emerge within the next 5 years, the policy and operational means developed to combat them, the main active stakeholders and the EU legislation in force. In this context, a short history of EU research on security and defence is presented, followed by an inventory of relevant research and development projects funded under the Horizon 2020 framework programme during the period 2014-2018. The specific contributions of the Joint Research Centre to security research are also highlighted. Finally, future avenues for security and defence research and development are discussed.

Please note that the executive summary of this landscape report has been published simultaneously as a companion document.

Acknowledgements

This report has been produced under the lead of the Knowledge for Security and Migration Unit (JRC.E7; Head of Unit, Giampiero Tartaglia).

Editorial team

Guy Bordin, Mayya Hristova and Encarnacion Luque-Perez

Contributors

Darina Blagoeva – Knowledge for the Energy Union Unit (JRC.C7)

Guy Bordin - Knowledge for Security & Migration Unit (JRC.E7)

Yuri Bruinen de Bruin - Knowledge for Security & Migration Unit (JRC.E7)

Constantin Ciupagea –Land Resources Unit (JRC.D3)

Sorin Cursaru - Knowledge for Security & Migration Unit (JRC.E7)

Guido Ferraro – Transport and Border Security Unit (JRC.E5)

Massimo Flore - Knowledge for Security & Migration Unit (JRC.E7)

Georgios Giannopoulos – Technology Innovation in Security Unit (JRC.E2)

Harm Greidanus - Knowledge for Security & Migration Unit (JRC.E7)

Mayya Hristova - Knowledge for Security & Migration Unit (JRC.E7)

Maciej Krzysztofowicz – Foresight, Modelling, Behavioural Insights & Design for Policy Unit (JRC.I2)

Martin Larcher – Safety and Security of Buildings Unit (JRC.E4)

Anne Sophie Lequarre - Knowledge for Security & Migration Unit (JRC.E7)

Encarnacion Luque-Perez - Knowledge for Security & Migration Unit (JRC.E7)

Marcelo Masera - Energy Security, Distribution and Markets Unit (JRC.C3)

Igor Nai Fovino – Cyber & Digital Citizens' Security Unit (JRC.E3)

Franco Oliveri – Transport and Border Security Unit (JRC.E5)

Claudiu Pavel – Knowledge for the Energy Union Unit (JRC.C7)

Gianluigi Ruzzante - Knowledge for Security & Migration Unit (JRC.E7)

George Solomos – Safety and Security of Buildings Unit (JRC.E4)

Desislava Strezova – Safety and Security of Buildings Unit (JRC.E4)

Giampiero Tartaglia - Knowledge for Security & Migration Unit (JRC.E7)

Marianthi Theocharidou – Technology Innovation in Security Unit (JRC.E2)

Ana Lisa Vetere Arellano - Knowledge for Security & Migration Unit (JRC.E7)

Executive summary

The aim of this report is to provide in a single document a large landscape review of the security and defence research and development in the European Union. For this purpose, it dedicates a substantive part of its content to set the scene, i.e., understanding the security threats currently observed and expected to arise in the next years, listing the policy initiatives and strategies for combating them, presenting the main stakeholders and the relevant legislation in the field. This part is organised around several thematic ‘building blocks’ – border control; critical infrastructure protection; public space protection; critical supplies security; cybersecurity; chemical, biological, radiological, nuclear and high-yield explosive threats; hybrid threats; combating radicalisation to terrorism; fighting against terrorism financing; space; and defence – under the umbrella of the three core priorities defined in the European agenda on security: terrorism, organised crime and cybercrime.

The picture is completed by presenting the history and evolution of the security and defence research and development funding of the European Union. In this context, all the R&D projects funded under the Horizon 2020 framework programme during the period 2014-2018 were analysed in order to identify those related to security and defence, allocate them to the various building blocks and priorities mentioned above. A basic statistical analysis gives information about the number of projects, funding programme, country participation and dual-use potential. The latter is considered from the perspective of Horizon 2020 projects with civil applications which could also be used in the defence sector. The specific contributions of the Joint Research Centre to security and defence research are also highlighted.

The analysis of the 349 security and defence Horizon 2020 R&D projects shows that almost half of them are related to cybersecurity. There are also a significant number of projects that are multi-thematic, i.e. related to two or more building blocks (21%) or to two or more priorities (11%). The analysis also illustrates that the specific Horizon 2020 programme dedicated to security is not the only funding source for projects displaying security component as 41% of them are funded by other Horizon 2020 programmes. Regarding the involvement of the EU Member States, all of them are contributors (as participant or coordinator) of one project at least, but five of them stand out – the UK, Spain, Italy, Germany and France – accounting for 56% of the total EU contributors. Considering the legal status of the contributors, private-for-profit companies represent a very high share, 48% of the total. They are also predominant among the coordinators of projects. However, private for-profit companies are much less involved in projects related to combating radicalisation, while public bodies’ contribution is particularly low in the area of cybersecurity. The analysis shows further that the overwhelming majority (approx. 90%) of the considered research projects have potential dual-use applications, i.e. their output with civil application could also be used in the defence sector.

Finally, future avenues for security and defence research and development are discussed by building block, with the discussion being complemented by more specific foresight insights gathered from a topical horizon-scanning exercise carried out at the Joint Research Centre. Its results hint on the relative importance of “life sciences” for the future and the attention that need to be put on the growing role of manipulations of the living, which raises all kinds of concern, also in terms of security.

This landscape report is meant to be the base for an online living document, which could be updated with new data (e.g. relevant legislation, analysis of R&D projects or results of foresight exercises) when appropriate. A potential avenue for future development would be the analysis of EU funded R&D projects in terms of achieved output and impact on society at large (e.g. innovation, policy development, knowledge transfer and dissemination, etc.), once the H2020 framework programme will be completed. Another dimension of future deeper analysis is the dual-use potential of such projects. This latter analysis is on the way of being undertaken by the editorial team of this report and should be available early 2020.

1 Introduction

Living in peace and security was a founding principle for establishing in the 1950s the first nucleus of what would eventually become the European Union. This is indeed a condition for any society to develop, for the sake of all its members. Therefore, security has also been a major focus of the 2014-2019 European Commission from the very beginning of its mandate. Furthermore, the dramatic series of terrorist attacks that hit several European countries from 2015 onwards have increased the challenges faced by the EU (and the whole world) in this area, making security issues a top priority. In addition, recent development in world geopolitics and the growing overlap between civilian and military operations have increased the EU's strategic interest in defence. The primary areas of this interest lie in the development of a defence industry for growth and cost saving, the establishment of territorial defence, the exploitation of military capacity for civil protection and security, and ensuring that the EU maintains its role as a global actor. Above all, the goal remains to protect and defend EU citizens, EU values and the EU way of life, based on ethics, integrity, freedom and respect for human rights.

By March 2019, 28 legislative initiatives related to security had been presented, of which 19 had been agreed by the European Parliament and the Council of the European Union, while 9 were still on the table for the agreement of both institutions ⁽¹⁾.

It comes out that the 2019-2024 European Commission will immediately face the security and defence file. The main new challenges include, in particular, a stronger call for a Commission role in defence, owing to the evolution of security threats inside and around Europe; the effect of globalisation, which has deepened interconnections between Europe and the rest of the world; and dependence on complex, interdependent infrastructures. Further drivers are the blurring of the distinction between internal and external security, the shifting geopolitical landscape and technological developments that have introduced benefits but also new risks and dependencies. As a consequence, the security and defence reality is constantly evolving, potentially confronted to conventional, non-conventional and irregular warfare, cyberthreats and fake news; that has resulted in a shift of emphasis from targeted security to ensuring the resilience of structures, processes and citizens.

To support these major trends and priorities, research on security and defence is much needed, and it has consequently gained in importance under EU research schemes. Parts of the Horizon 2020 (H2020) framework programme for research and innovation are dedicated to security research (and it was part of the previous seventh framework programme for research and innovation (FP7), while defence research has mainly been undertaken so far by national actors, with some limited collaboration between EU Member States. The EU has, however, not been left behind in this regard. In particular, in its report *A New Deal For European Defence* ⁽²⁾, the European Commission focused specifically on dual-use research and in particular the maximisation of synergies between the civil research included in H2020 and the defence research activities coordinated by the European Defence Agency (EDA).

Objective and content

In this context, the main objective of this report is to provide information about the current situation with regard to EU-funded research aimed at supporting EU security and defence policymaking, focusing exclusively on man-made risks and threats intended to harm individuals and societies at large.

For this purpose, a multi-step approach has been followed. Chapter 2 provides a comprehensive overview of the security and defence situation in the EU. This overview is organised around several thematic building blocks (namely border control; critical infrastructure protection; public space protection; critical supplies security; cybersecurity; chemical, biological, radiological, nuclear and high-yield explosive threats (CBRN-E); hybrid threats; combating radicalisation to terrorism; fighting against terrorism financing; space; and defence), under the umbrella of the three core priorities defined in the European agenda on security: terrorism, organised crime and cybercrime.

For each building block, the chapter includes (i) a review of the main current risks and threats; (ii) a description of the scene in the EU (and beyond where relevant) in terms of policy spheres and practical/operational implementation; (iii) a prospective review of the risks and threats expected to emerge

⁽¹⁾ 22 (15 agreed + 7 pending) under the Security Union initiative, 6 (4 agreed + 2 pending) under other Commission initiatives having security components; see European Commission Communication COM(2019) 145 final, and European Agenda on Security – Factsheet Delivering on the Security Union (20 March 2019) available at https://ec.europa.eu/home-affairs/what-we-do/policies/european-agenda-security/fact-sheets_en; consulted on 10 April 2019.

⁽²⁾ European Commission, Commission report, *A New Deal for European Defence* (COM(2014) 387 final), Brussels, 24.6.2014.

within the next 5 years; (iv) a description of main EU and international actors active in a particular field, and their responsibilities and capacities; and (v) a list of EU legislation in force and of other reference documents at EU and international levels.

Chapter 3 starts with a short history of EU research on security and defence, before reviewing the recent and current research projects funded through the H2020 framework programme. An inventory of relevant projects covering the period 2014-2018 has been carried out, allowing a statistical analysis to be performed, looking at, for example, the distribution of the projects by building block, core priority, H2020 research programme and country involved. As a consequence of the growing overlap between civil and defence domains, the dual-use nature of projects has also been examined. This chapter also describes the specific contributions of the Joint Research Centre (JRC) to the various building blocks. All in all, this study constitutes the first analysis of this type performed on EU security and defence research projects ⁽³⁾.

Finally, in Chapter 4, future avenues for security and defence research and development (R & D) in the EU are discussed, by building block and based on the above information. This chapter benefits from foresight perspectives gathered from a horizon-scanning exercise on security and defence carried out at the JRC.

Please note that this report need not be read from cover to cover. In fact, it has been designed to allow thematic reading (by building block), which may better satisfy the reader's interest.

Expected impact

The authors hope that the report will support the work of the new European Commission (2019-2024) and the EU policy makers in the domain of security and defence. Its holistic approach should help in identifying the main issues, the gaps and uncovered fields, the links between threats, and areas that have dual-use potential, as well as providing insights into expected developments in the next 5 years and beyond. The ultimate goal and the expected impact of the report are that it will help to shape future EU R & D in security and defence.

⁽³⁾ An impact analysis of these research projects (e.g. looking at their impact on EU policymaking) has not been carried out for the sake of this landscape study, as it will be possible to estimate their impact with any degree of certainty only once the H2020 framework programme and its funded projects are over.

2 The security and defence situation in the European Union

This chapter provides an overview of the security and defence situation in the EU, including (i) a review of main risks and threats currently existing, (ii) a description of the EU scene (and beyond when relevant) in terms of policy spheres and practical/operational implementations, (iii) a prospective review of the risks and threats suspected to emerge within the next five years, (iv) a description of main EU and international actors active in a particular field, their responsibilities and capacities, and (v) a list of EU policies in force and other reference documents, both at EU and international levels. To ease the presentation of information, this overview is organised around several thematic building blocks – border control; critical infrastructure protection; public space protection; critical supplies security; cybersecurity; CBRN-E; hybrid threats; combating radicalisation to terrorism; fighting against terrorism financing; space; and defence.

2.1 Border control

2.1.1 What is border control?

Within the EU, border control is defined as the activities carried out at the EU's external borders in accordance with and for the purposes of Regulation (EU) 2016/399 (the Schengen Borders Code) ⁽⁴⁾, exclusively in response to an intention to cross or the act of crossing that border, regardless of any other consideration, consisting of border checks and border surveillance.

Border control is a very broad and complex area, with many stakeholders interacting on its three main dimensions: land, air and sea.

Moreover, recent developments have introduced a fourth dimension: the cyber-border. Concerns stemming from the convergence of border and cybersecurity threats are nothing new to those involved in both disciplines. Criminals and foreign actors have been exploiting computers and cyber methods to circumvent physical border security for decades. Today, nearly every crime or security threat that once required some physical nexus with the nation's traditional borders (land, air and sea) is being committed, or at least facilitated, by some cyber component. In many ways, vulnerabilities in cybersecurity render some aspects of traditional border security irrelevant or, at the very least, much less effective (Osborn, 2017).

Recent major events, such as the 2015 crisis in migration to Europe, make border control an increasingly essential element in the security domain, as well as in the general public perception of EU citizens of the performance of the EU as a whole.

Two political developments that are of particular relevance to border control are the European agenda on migration and the European agenda on security.

The European agenda on migration ⁽⁵⁾ includes the following initiatives:

- a revised proposal for an entry–exit system ⁽⁶⁾ to facilitate and reinforce border check procedures for non-EU nationals;
- the proposed reform of the Common European Asylum System, including the Dublin regulation, the European Union Agency for Asylum, the asylum procedures regulation, the qualification regulation, the reception conditions directive and the EU resettlement framework;
- a proposal to adapt and reinforce the European Asylum Dactyloscopy Database (Eurodac) system, with a view to facilitating returns and helping tackle irregular migration;
- a proposal for a targeted modification to the Schengen Borders Code to make checks on EU citizens against all relevant databases mandatory;
- the implementation of the EU action plan against migrant smuggling (2015-2020);
- an EU action plan on return;

⁽⁴⁾ Regulation (EU) 2016/399 of the European Parliament and of the Council of 9 March 2016 on a Union Code on the rules governing the movement of persons across borders (Schengen Borders Code), OJ L 77, 23.3.2016, p. 1-52.

⁽⁵⁾ European Commission, Commission communication, 'A European agenda on migration' (COM(2015) 240 final), Brussels, 13.5.2015.

⁽⁶⁾ European Commission, Commission communication, 'Proposal for a regulation establishing an entry/exit System (EES) to register entry and exit data and refusal of entry data of third country nationals crossing the external borders of the Member States of the European Union and determining the conditions for access to the EES for law enforcement purposes and amending Regulation (EC) No 767/2008 and Regulation (EU) No 1077/2011' (COM(2016) 194 final), Brussels, 6.4.16.

— a detailed ‘Back to Schengen’ roadmap.

The key aspects of the European agenda on security include ⁽⁷⁾:

- a proposal for the European Travel Information and Authorisation System (ETIAS) to strengthen security checks on visa-free travellers ⁽⁸⁾, with the ETIAS Central Unit envisaged as part of the European Border and Coast Guard Agency (Frontex), and the implementation of the system, once adopted, requiring close interagency cooperation, particularly between the European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA), Frontex and the European Union Agency for Law Enforcement Cooperation (Europol);
- the establishment of the High-Level Expert Group on Information Systems and Interoperability, with the participation of Frontex, Europol, eu-LISA and other EU agencies;
- the adoption of the EU passenger name records (PNR) directive ⁽⁹⁾ and the EU PNR implementation plan;
- proposals to revise the Schengen Information System (SIS) ⁽¹⁰⁾, aiming to enhance the ability of the system to fight terrorism and cross-border crime, improve border and migration management and ensure an effective information exchange between Member States.

2.1.2 A political priority of the European Commission

Border control is very high on the EU's political agenda. In the European Commission's political guidelines issued in 2014 ⁽¹¹⁾, border control is an intrinsic component of at least two priorities:

1. **An area of justice and fundamental rights based on mutual trust.** The document states, ‘Combating cross-border crime and terrorism is a common European responsibility. We need to crack down on organised crime, such as human trafficking, smuggling and cybercrime. We must tackle corruption; and we must fight terrorism and counter radicalisation — all the while guaranteeing fundamental rights and values, including procedural rights and the protection of personal data.’
2. **Towards a new policy on migration.** The document mentions the common asylum policy and a new migration policy but also the need to secure Europe's borders. This entails a need to step up the operational capacities of Frontex.

President Jean-Claude Juncker's State of the Union Address 2017 acknowledged the progress made in these areas: ‘We are now protecting Europe's external borders more effectively. Over 1 700 officers from the new European Border and Coast Guard are now helping Member States’ 100 000 national border guards patrol in places like Greece, Italy, Bulgaria and Spain. ... We have managed to stem irregular flows of migrants, which were a cause of great anxiety for many. ... In doing so, we have drastically reduced the loss of life in the Mediterranean’ ⁽¹²⁾.

At the same time, the speech also emphasised the need to better counter cross-border terrorist threats and further strengthen the external borders, by opening the Schengen area to Romania and Bulgaria.

⁽⁷⁾ European Commission, Commission communication, ‘The European agenda on security’ (COM(2015) 185 final), Strasbourg, 28.4.2015.

⁽⁸⁾ European Commission, Commission communication, ‘Proposal for a Regulation establishing a European Travel Information and Authorisation System (ETIAS) and amending Regulations (EU) No 515/2014, (EU) 2016/399, (EU) 2016/794 and (EU)2016/1624’ (COM(2016) 731 final), Brussels, 16.11.2016.

⁽⁹⁾ Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, OJ L 119, 4.5.2016, p. 132-149.

⁽¹⁰⁾ European Commission, Commission communication, ‘Proposal for a Regulation of the European Parliament and of the Council on the establishment, operation and use of the Schengen Information System (SIS) in the field of border checks, amending Regulation (EU) No 515/2014 and repealing Regulation (EC) No 1987/2006’ (COM(2016) 882 final), Brussels, 21.12.2016.

⁽¹¹⁾ European Commission, *A New Start for Europe: My agenda for jobs, growth, fairness and democratic change*, (https://ec.europa.eu/commission/sites/beta-political/files/juncker-political-guidelines-speech_en.pdf).

⁽¹²⁾ European Commission, ‘President Jean-Claude Juncker's State of the Union Address 2017’ (http://europa.eu/rapid/press-release_SPEECH-17-3165_en.htm).

2.1.3 The possible evolution of border control within the next 5 to 10 years

The Commission's proposal for the multiannual financial framework (MFF) for 2021-2027 was released in May 2018 ⁽¹³⁾. The document confirms that the strengthening of the external borders remains a high priority for the European Commission. It states: 'the effective protection of our external borders is a prerequisite for ensuring a safe area for the free movement of persons and goods within the Union. This includes the proper management of flows of persons and goods and safeguarding the integrity of the customs union. A new integrated Border Management Fund will provide vital and reinforced support to Member States in the shared responsibility of securing the common external borders of the Union. The Fund will cover border management, visas and customs control equipment. It will help ensure equivalence in the performance of customs controls at the external borders. This will be achieved by addressing the current imbalances between Member States due to geographical, capacity and resource differences. This will not only strengthen customs controls but also facilitate legitimate trade, contributing to a secure and efficient customs union' ⁽¹⁴⁾.

These efforts need to be complemented by a strong and fully operational European Border and Coast Guard Agency (Frontex) at the core of a fully integrated EU border management system. The Commission proposes to create a standing corps of around 10 000 border guards by the end of the financial period. It will also provide financial support and training for national border guards in Member States. This will enable the stepping up of operational capacity, the reinforcement of existing tools and the development of EU-wide information systems for borders, migration management and security ⁽¹⁵⁾.

The proposal is for the EU budget for the management of external borders, migration and refugee flows to be significantly reinforced, totalling nearly EUR 33 billion, compared with EUR 12.4 billion for the period 2014-2020.

2.1.4 Stakeholders

2.1.4.1 European Union stakeholders

European Commission Directorate-General for Migration and Home Affairs

The Directorate-General (DG) for Migration and Home Affairs is in charge of the policy area known as migration and home affairs. It works to develop a balanced and comprehensive EU migration policy, based on solidarity and responsibility, which — in line with the Europe 2020 strategy — will make an important contribution to the EU's economic development and performance in the longer term. Its aim is to create an EU-wide set of rules for legal migration while taking into account the interconnection between migration and integration. It also aims to address irregular migration and trafficking in human beings. At the same time, it works to set up a Common European Asylum System, based on solidarity and respect for fundamental rights, to ensure effective protection for the people who need it.

DG Migration and Home Affairs helps build a safer Europe by fighting terrorism and organised crime, by promoting police cooperation and by preparing to respond swiftly to emerging crises. The DG's actions in these areas include stricter rules against illicit trafficking of firearms and on trafficking in human beings, as well as revision of legislation on combating child sexual abuse, sexual exploitation and child pornography. The fight against terrorism and the internal security strategy, strictly linked to the broader European security strategy, will continue to be cornerstones of its efforts to make Europe more secure by strengthening cooperation on law enforcement, border management, civil protection and disaster management.

In all these areas, DG Migration and Home Affairs promotes dialogue and cooperation with non-EU countries so that we can work in partnership and jointly tackle common challenges. Its external action contributes to the strengthening of the EU's position as a reliable, active and pragmatic global player.

https://ec.europa.eu/home-affairs/index_en

⁽¹³⁾ European Commission, Commission communication, 'A modern budget for a union that protects, empowers and defends: The multiannual financial framework for 2021-2027' (COM(2018) 321 final), Brussels, 2.5.2018.

⁽¹⁴⁾ European Commission communication COM(2018) 321 final.

⁽¹⁵⁾ European Commission, Commission communication, 'Proposal for a Regulation on the European Border and Coast Guard and repealing Council Joint Action No 98/700/JHA, Regulation (EU) No 1052/2013 of the European Parliament and of the Council and Regulation (EU) No 2016/1624 of the European Parliament and of the Council' (COM(2018) 631 final), Brussels, 12.9.2018.

European Commission Directorate-General Joint Research Centre

As the European Commission's science and knowledge service, the JRC supports EU policies with independent scientific evidence throughout the whole policy cycle.

Since January 2014, the JRC has supported DG Migration and Home Affairs in its policies regarding border control, in particular in the development of the European Border Surveillance System (Eurosir) ⁽¹⁶⁾ and in analysing innovative solutions for border surveillance. More details are presented in Section 3.4.

Since 2010, under a series of administrative arrangements with the Directorate-General for Maritime Affairs and Fisheries, the JRC (through its Transport and Border Security Unit) has collaborated with other relevant DGs and agencies to support the design and implementation of the Common Information Sharing Environment (CISE) for maritime surveillance, which is one of the pillars of the European Union maritime security strategy (EUMSS) for the global maritime domain, and hence a crucial part of blue border surveillance.

https://ec.europa.eu/info/departments/joint-research-centre_en

European Border and Coast Guard Agency (Frontex)

The mission of Frontex is to promote, coordinate and develop European border management in line with the EU Charter of Fundamental Rights and the concept of integrated border management.

To help identify migratory patterns as well as trends in cross-border criminal activities, Frontex analyses data related to the situation at and beyond the EU's external borders. It monitors the situation at the borders and helps border authorities to share information with EU Member States. The agency also carries out vulnerability assessments to evaluate the capacity and readiness of each Member State to face challenges at its external borders, including migratory pressure.

Frontex coordinates and organises joint operations and rapid border interventions to assist Member States at the external borders, including in humanitarian emergencies and for rescue at sea. The agency deploys European Border and Coast Guard teams, including a pool of at least 1 500 border guards and other relevant staff, in rapid interventions. The members of this pool must be provided by Member States upon request by the agency. It also deploys vessels, aircraft, vehicles and other technical equipment provided by Member States in its operations. In addition, Frontex may carry out operations on the territory of non-EU countries neighbouring at least one Member State, where there is migratory pressure at a non-EU country's border.

Frontex supports Member States with screening, debriefing, identification and fingerprinting of migrants. Officers deployed by the agency refer and provide initial information to people who need, or wish to apply for, international protection, cooperating with the European Asylum Support Office (EASO) and national authorities. National authorities, not Frontex, decide who is entitled to international protection. The agency also assists Member States with forced returns of people who have exhausted all legal avenues to legitimise their stay within the EU. This help includes obtaining travel documents for returnees by working closely with the consular authorities of the relevant non-EU countries.

Frontex focuses on preventing smuggling, human trafficking and terrorism as well as many other cross-border crimes. It shares any relevant intelligence gathered during its operations with relevant national authorities and Europol. The agency is a centre of expertise in the area of border control. It develops training curricula and specialised courses in a variety of areas to guarantee the highest levels of professional knowledge among border guards across Europe. It also supports search and rescue operations that arise during border surveillance operations at sea.

<https://frontex.europa.eu/>

European Maritime Safety Agency (EMSA)

EMSA is one of the EU's decentralised agencies. Based in Lisbon, the Agency provides technical assistance and support to the European Commission and EU Member States in the development and implementation of EU legislation on maritime safety, pollution by ships and maritime security. It has also been given operational tasks in the field of oil pollution response, vessel monitoring and long-range identification and tracking of vessels.

<http://www.emsa.europa.eu/>

⁽¹⁶⁾ Regulation (EU) No 1052/2013 of the European Parliament and of the Council of 22 October 2013 establishing the European Border Surveillance System (Eurosir), OJ L 295, 6.11.2013, p. 11-26.

European Asylum Support Office

EASO is the EU agency that supports the implementation of a Common European Asylum System by applying a bottom-up approach. The aim is to ensure that individual asylum cases are dealt with in a consistent way by all Member States.

EASO provides different kinds of support, including, in particular, supporting and stimulating the common quality of the asylum process, tailored assistance, emergency support for Member States subject to particular pressures, sharing and merging information and data, and support to non-EU countries.

<https://www.easo.europa.eu/>

European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice

eu-LISA was established to provide a long-term solution for the operational management of large-scale IT systems, which are essential instruments in the implementation of the asylum, border management and migration policies of the EU.

The agency currently manages Eurodac, the second generation Schengen Information System (SIS II) and the Visa Information System (VIS).

<https://www.eulisa.europa.eu/>

European Union Agency for Law Enforcement Cooperation (Europol)

Europol is the EU's law enforcement agency. Its main goal is to achieve a safer Europe, supporting the EU Member States in their fight against terrorism, cybercrime and other serious and organised forms of crime. It also works with many non-EU partner states and international organisations. Some of the services provided by Europol are listed below.

- **Operational coordination and support.** The Operational Centre (running 24/7) is the hub for the exchange of data among Europol, EU Member States and third parties on criminal activity.
- **Information exchange.** There are three systems in place for information exchange: (i) the Secure Information Exchange Network Application (SIENA) is a platform that meets the communication needs of EU law enforcement; (ii) the Europol Information System is Europol's central criminal information and intelligence database, covering all of Europol's mandated crime areas, including terrorism; and (iii) the Europol Platform for Experts is a collaborative web platform for specialists in a variety of law enforcement areas that facilitates the sharing of best practices, documentation, knowledge and non-personal data on crime.
- **Strategic analysis.** Europol does this to help decision-makers identify priorities in the fight against organised crime and terrorism. Once this has been done, law enforcement officers can tailor their operational work nationally, regionally and locally.
- **Intelligence analysis**
 - Cyber intelligence involves collecting, processing and analysing information on cybercrime (from a wide array of public, private and open sources).
 - Cyber community engagement — the European Cybercrime Centre (EC3) develops and maintains partnerships to support the response of EU Member States to cybercrime. It carries out research on internet governance to pinpoint significant vulnerabilities that organised crime groups can exploit.
- **Forensics.** Europol provides forensic support to law enforcement agencies across the EU, in relation to crimes that include euro counterfeiting, illicit drug production, payment card fraud and cybercrime.
- **Training and capacity building.** EC3 supports EU Member States' law enforcement authorities through capacity building and training, links available EU funding with law enforcement partners and acts as a central host for hi-tech services to support national investigations.
- **Joint investigation teams.** These are investigative teams set up for a fixed period and specific purpose, based on an agreement between law enforcement authorities in EU Member States (non-EU countries may participate with the agreement of all other participants).

- **Joint Cybercrime Action Taskforce.** The taskforce's objective is to drive intelligence-led, coordinated action against key cybercrime threats and targets by facilitating the joint identification, prioritisation, preparation and initiation of cross-border investigations and operations by its partners.

<https://www.europol.europa.eu/>

European External Action Service (EEAS)

The EEAS is the EU's diplomatic service. It helps the EU's foreign affairs chief — the High Representative of the Union for Foreign Affairs and Security Policy and Vice-President of the Commission (HR/VP) — to implement the EU's common foreign and security policy (CFSP).

A key aspect of the EEAS's activities is its ability to work closely with the foreign and defence ministries of the EU Member States and with EU institutions. It also has a strong working relationship with the United Nations and other international organisations.

Following the Treaty of Lisbon, the EEAS is responsible for the running of EU delegations and offices around the world. The 139 delegations play a vital role in representing the EU and its citizens around the globe and in building networks and partnerships. Their main role is to represent the EU in the country where they are based and to promote the values and interests of the EU.

<https://eeas.europa.eu>

2.1.4.2 International stakeholders

North Atlantic Treaty Organization (NATO)

On 8 July 2016, the President of the European Council and the President of the European Commission, together with the Secretary General of NATO, signed a joint declaration in Warsaw with a view to giving new impetus and new substance to the EU–NATO strategic partnership ⁽¹⁷⁾.

One of the seven specific areas where cooperation is to be enhanced is operational cooperation, including at sea and on migration.

2.1.5 Legislation and reference documents

- Council Directive 2004/82/EC of 29 April 2004 on the obligation of carriers to communicate passenger data, OJ L 261, 6.8.2004, p. 24-27.
- Regulation (EC) No 1987/2006 of the European Parliament and of the Council of 20 December 2006 on the establishment, operation and use of the second generation Schengen Information System (SIS II), OJ L 381, 28.12.2006, p. 4-23.
- Regulation (EC) No 767/2008 of the European Parliament and of the Council of 9 July 2008 concerning the Visa Information System (VIS) and the exchange of data between Member States on short-stay visas (VIS Regulation), OJ L 218, 13.8.2008, p. 60-81.
- Regulation (EC) No 810/2009, of the European Parliament and of the Council of 13 July 2009 establishing a Community Code on Visas (Visa Code), OJ L 243, 15.9.2009, p. 1-58.
- Regulation (EU) No 603/2013 of the European Parliament and of the Council of 26 June 2013 on the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of Regulation (EU) No 604/2013 establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person and on requests for the comparison with Eurodac data by Member States' law enforcement authorities and Europol for law enforcement purposes, and amending Regulation (EU) No 1077/2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice, OJ L 180, 29.6.2013, p. 1-30.
- Regulation (EU) No 1052/2013 of the European Parliament and of the Council of 22 October 2013 establishing the European Border Surveillance System (Eurosir), OJ L 295, 6.11.2013, p. 11-26.

⁽¹⁷⁾ EEAS, 'EU–NATO cooperation — factsheets' (https://eeas.europa.eu/headquarters/headquarters-homepage/28286/eu-nato-cooperation-factsheet_en).

- Regulation (EU) No 515/2014 of the European Parliament and of the Council of 16 April 2014 establishing, as part of the Internal Security Fund, the instrument for financial support for external borders and visa and repealing Decision No 574/2007/EC, OJ L 150, 20.5.2014, p. 143-167.
- Regulation (EU) No 656/2014 of the European Parliament and of the Council of 15 May 2014 establishing rules for the surveillance of the external sea borders in the context of operational cooperation coordinated by the European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union, OJ L 189, 27.6.2014, p. 93-107.
- Regulation (EU) 2016/399 of the European Parliament and of the Council of 9 March 2016 on a Union Code on the rules governing the movement of persons across borders (Schengen Borders Code), OJ L 77, 23.3.2016, p. 1-52.
- Directive (EU) 2016/681 of the European Parliament and of the Council of 9 March 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, OJ L 119, 4.5.2016, p. 132-149.
- Regulation (EU) 2016/1624 of the European Parliament and of the Council of 14 September 2016 on the European Border and Coast Guard and amending Regulation (EU) 2016/399 of the European Parliament and of the Council and repealing Regulation (EC) No 863/2007 of the European Parliament and of the Council, Council Regulation (EC) No 2007/2004 and Council Decision 2005/267/EC, OJ L 251, 16.9.2016, p. 1-76.
- Regulation (EU) 2016/1625 of the European Parliament and of the Council of 14 September 2016 amending Regulation (EC) No 1406/2002 establishing a European Maritime Safety Agency, OJ L 251, 16.9.2016, p. 77-79.
- Regulation (EU) 2016/1626 of the European Parliament and of the Council of 14 September 2016 amending Regulation (EC) No 768/2005 establishing a Community Fisheries Control Agency, OJ L 251, 16.9.2016, p. 80-82.
- Council of the European Union, Council conclusions on the revision of the European Union maritime security strategy (EUMSS) Action Plan (10494/18), Brussels, 26 June 2018.

2.2 Critical infrastructure protection

2.2.1 What is a critical infrastructure?

Although there is no single definition of what a critical infrastructure is, all definitions underline the detrimental effects that the disruption or destruction of such a critical infrastructure would have on society. Several examples of definitions from around the world illustrate this ⁽¹⁸⁾. For instance, in the United States of America, the Patriot Act of 2001 defines critical infrastructure as those ‘systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters’ ⁽¹⁹⁾. In Canada, critical infrastructure refers to ‘processes, systems, facilities, technologies, networks, assets and services essential to the health, safety, security or economic well-being of Canadians and the effective functioning of government. Critical infrastructure can be stand-alone or interconnected and interdependent within and across provinces, territories and national borders. Disruptions of critical infrastructure could result in catastrophic loss of life, adverse economic effects and significant harm to public confidence’ ⁽²⁰⁾. In Switzerland, ‘critical infrastructure protection aims to ensure the supply of crucial goods and services, such as energy, transport and healthcare. Critical infrastructures include not just buildings and facilities, but also supply systems and services in the broadest sense. Serious disruptions, for example, a nationwide power cut, can have far-reaching consequences for the population and cause considerable damage to the economy’ ⁽²¹⁾.

⁽¹⁸⁾ For a complete list of definitions, see CIPedia, an online glossary of multinational definitions related to critical infrastructure protection (<http://www.cipedia.eu>).

⁽¹⁹⁾ US 107th Congress, Public Law 56, Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001.

⁽²⁰⁾ Public Safety Canada, ‘Critical infrastructure’ (<https://www.publicsafety.gc.ca/cnt/ntnl-scrtr/crtcl-nfrstrctr/index-en.aspx>).

⁽²¹⁾ Swiss Federal Office for Civil Protection, ‘Critical infrastructures’ (<https://www.babs.admin.ch/en/aufgabenbabs/ski/kritisch.html>).

In the EU, a Green Paper adopted in 2005 on a European programme for critical infrastructure protection (EPCIP) ⁽²²⁾ understood it as ‘the ability to prepare for, protect against, mitigate, respond to, and recover from critical infrastructure disruptions or destruction’. In this document, critical infrastructures include ‘those physical resources, services, and information technology facilities, networks and infrastructure assets which, if disrupted or destroyed, would have a serious impact on the health, safety, security or economic well-being of citizens or the effective functioning of governments’. It also defines European critical infrastructure (ECI) as that which upon disruption or destruction would have a significant impact on at least two Member States. A total of 11 sectors with 37 subsectors were identified as critical infrastructure sectors: energy, information and communication technology (ICT), water, food, health, finance, public and legal order and safety, civil administration, transport, chemical and nuclear industry, and space and research.

One year later, a Commission communication ⁽²³⁾ set out the principles, processes and instruments proposed to implement EPCIP.

Then, in 2008, a Council directive on ECI ⁽²⁴⁾ was adopted to implement EPCIP. This directive applies, however, only to the energy and transport sectors, further divided into three energy subsectors (electricity, oil and gas) and five transport subsectors (road, rail, air, inland waterways, and ocean and short sea shipping and ports) ⁽²⁵⁾.

In 2016, another directive fostered increased security levels in networks and information systems ⁽²⁶⁾. The directive attempts to establish a culture of security across sectors that are vital for the economy and society and, moreover, rely heavily on ICT, such as energy, transport, water, banking, financial market infrastructures, healthcare and digital infrastructure. Businesses in these sectors that are identified by the Member States as operators of essential services have to take appropriate security measures and notify serious incidents to the relevant national authority.

2.2.2 Threats to critical infrastructures

Reducing the vulnerabilities of critical infrastructures and increasing their resilience ⁽²⁷⁾ to threats is one of the major objectives of the EU. In particular, adequate protection must be ensured and detrimental effects of disruption and destruction on society and people must be contained as far as possible.

Threats to critical infrastructures are multiple and can be caused intentionally or unintentionally. Critical infrastructures can be damaged, disrupted or destroyed by deliberate acts of terrorism, criminal activity, computer hacking, malicious behaviour, negligence, accidents and natural disasters.

It must, however, be underlined that besides these deliberate or accidental disruptions, there are other factors that reinforce overall critical infrastructure-related risks. Examples of such factors are (Setola et al., 2016): (1) a reduction in state/public control as a result of liberalisation and privatisation of infrastructures; (2) increased use of information and telecommunication technologies to support, monitor and control critical infrastructure functionalities; (3) the idea on the part of the population that services can and will be available 24/7, meaning that acceptance of critical infrastructure failure has become very low, thus making protection a higher priority than it was in the 1980s; (4) urbanisation, which pushes the utilisation of ageing infrastructures to the limit; (5) the increasing interwovenness, (supply) chaining and dependencies of infrastructural services; and (6) the increasing understanding on the part of various adversaries of society that a successful attack may create societal havoc.

⁽²²⁾ European Commission, ‘Green Paper on a European programme for critical infrastructure protection’ (COM(2005) 576 final), Brussels, 17.11.2005.

⁽²³⁾ European Commission, Commission communication, ‘European Programme for Critical Infrastructure Protection’ (COM(2006) 786 final), Brussels, 12.12.2006.

⁽²⁴⁾ Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection, OJ L 345, 23.12.2008, p. 75-82.

⁽²⁵⁾ See Annex 1 for details. A comprehensive review of recent literature on infrastructure and related issues further categorises critical infrastructures into physical and social infrastructures (Kumari and Sharma, 2017). Note that in the present study most social infrastructures (e.g. shopping centres, healthcare facilities) are considered public spaces and therefore tackled in the relevant chapter.

⁽²⁶⁾ Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, OJ L 194, 19.7.2016, p. 1-30.

⁽²⁷⁾ There is no single definition of what ‘resilience’ means, but that proposed by Nan et al. (2016) applies well to critical infrastructures: ‘the ability of a system to resist the effects of disruptive forces and to reduce performance deviations’. See also, for example, Ouyang et al. (2012), Francis and Bekera (2014) and Setola et al. (2016). The UN Office for Disaster Risk Reduction defines ‘resilience’ as the ability of a system, community or society exposed to hazards to resist, absorb, accommodate, adapt to, transform and recover from the effects of a hazard in a timely and efficient manner, including through the preservation and restoration of its essential basic structures and functions through risk management (<https://www.unisdr.org/we/inform/terminology>).

Several of these aggravating factors, such as 1 and 4, are clearly dependent on political choices. Factor 5 is also to be noted. Critical infrastructures nowadays have a high degree of dependency and interdependency, on the one hand resulting in positive effects for society as a whole but on the other hand adding more complexity and hence more vulnerability to critical infrastructures and increased related risk. A lack of understanding of critical infrastructure dependencies, often non-intuitive or non-obvious, has been found to be highly problematic for the management of recent incidents ⁽²⁸⁾. Dependencies obviously constitute a major issue that has to be taken into consideration to a greater extent in critical infrastructure protection (Luijff et al., 2010; van Eeten et al., 2011; Setola et al., 2016; Setola and Theocharidou, 2016).

2.2.3 The European Union scene and beyond

EPCIP ⁽²⁹⁾ provides the framework for activities needed to improve the protection of critical infrastructures in the EU, throughout its Member States.

Practically, Directive 2008/114/EC 'establishes a procedure for the identification and designation of European critical infrastructures, and a common approach to the assessment of the need to improve the protection of such infrastructures in order to contribute to the protection of people' (Article 1). It also retains an 'all-hazards approach while countering threats from terrorism as a priority', meaning that 'man-made, technological threats and natural disasters should be taken into account in the critical infrastructure protection process, but the threat of terrorism should be given priority'. The key points of this directive are outlined below.

Identification and designation of ECI

- Each EU Member State identifies potential ECI, using cross-cutting criteria (e.g. possible casualties, economic effects and effect on people) and sectoral criteria specific to the type of ECI. Regular reviews must be carried out.
- Each EU Member State cooperates with other Member States with regard to potential ECI located on their territory.
- The directive applies only to the energy and transport sectors. In time, other sectors may be added.

Operator security plans

- Each EU Member State is to ensure that an operator security plan is in place for each ECI.
- This plan is to identify the critical assets of the ECI, as well as the existing security solutions for protecting them.

In addition, each EU Member State must ensure that a security liaison officer is designated for each ECI; the Member States also have to do specific and regular reporting to the Commission.

Following a comprehensive review ⁽³⁰⁾ of this directive, in 2013 the Commission adopted a new approach to EPCIP ⁽³¹⁾. It aims to build common tools and a common approach in the EU to critical infrastructure protection and resilience, taking better account of interdependencies between critical infrastructures, industries and state actors. This revised EPCIP takes a more pragmatic approach to the implementation of elements of risk assessment and risk management, focusing on case studies of European infrastructures (the Eurocontrol air traffic management system, the Galileo satellite system, the electricity transmission grid and the gas transmission network).

Within this policy context, the Commission has introduced a number of initiatives, in particular the European Reference Network for Critical Infrastructure Protection (ERNICIP), the Critical Infrastructure Preparedness and Resilience Research Network (CIPRNet) and the Critical Infrastructure Warning Information Network (CIWIN). They are discussed below in Sections 2.2.5 and 2.2.6.

⁽²⁸⁾ See Annex 2 for several examples of critical infrastructure disruption.

⁽²⁹⁾ European Commission Green Paper COM(2005) 576 final; European Commission communication COM(2006) 786 final.

⁽³⁰⁾ European Commission, Commission staff working document, 'Review of the European programme for critical infrastructure protection (EPCIP)' (SWD(2012) 190 final), Brussels, 22.6.2012.

⁽³¹⁾ European Commission, Commission staff working document, 'A new approach to the European programme for critical infrastructure protection: making European critical infrastructures more secure' (SWD(2013) 318 final), Brussels, 28.8.2013.

2.2.4 Possible evolution within the next 5 years

The landscape of critical infrastructure protection is rapidly evolving. What started back in the first decade of 2000 as an effort to ensure the protection of critical infrastructures assets has radically changed. Nowadays, the scientific community and critical infrastructure stakeholders are discussing the topics of resilience, interdependencies and a systems approach in order to improve the protection and resilience of critical infrastructures. It is expected that in the years to come discussion will be more about systems of critical infrastructures, even systems of systems, and how their interaction results in emerging behaviour that cannot be considered the sum of the performance of each interconnected infrastructure.

Another trend that is expected in the years to come is a shift in focus from protection to resilience. This reflects an increase in the number of threats and their complexity, such that threats cannot always be predicted and incorporated in a pure risk management approach. In this regard, it will be necessary to continue to develop resilience measures and to integrate them with existing and future security measures. As an example we mention the paradigm of hybrid threats, that is, complex attack vectors incorporating several methods: bolstering resilience is considered the main answer to this type of threat.

The paradigm of resilience is tightly linked to discussions about services and in particular continuity of critical services. The interconnectedness of critical infrastructures and the blurred boundaries between infrastructures have shifted attention to the services that infrastructures provide to citizens. This approach is increasingly being adopted by experts in the field and it is also reflected in the research work that is currently in full swing in Europe and elsewhere. The focus on services is also reflected in Directive (EU) 2016/1148.

The pervasiveness of ICT in all infrastructures has also created a new reality frequently referred to using the word 'smart'. Increasingly, the discussion is about 'smart grids', 'smart homes', etc., with the word 'smart' used to indicate that traditional infrastructures are nowadays integrated in such a pervasive manner with ICT that their nature has been completely altered. The internet of things (IoT) is driving changes in this area.

This digitalisation has led to more efficient infrastructures that provide better and more personalised services to citizens. At the same time, it has opened the door for new threats and vulnerabilities, with significant potential for cascade effects. Recent events have shown that these smart infrastructures may be less resilient than we believe. It is therefore natural that we will see in the near future a strong debate on the resilience versus efficiency issue. The two can be combined, but we need to break new ground in terms of the available knowledge. The aeronautical industry provides excellent examples of best practice in terms of how a system (air traffic management, aircraft, etc.) can be very efficient as well as resilient. To achieve this balance, better regulation, more research and better training of personnel may be required.

Furthermore, an area in which significant improvement is expected is training and education of stakeholders involved in critical infrastructure security and resilience. There is a common perception that the human factor is extremely important in the security chain. This is also related to the issue of insider threat, which seems to be a recurring problem for critical infrastructure stakeholders.

Cloud computing already has a strong footprint in the domain of critical infrastructures. Modern critical infrastructures are producing an enormous amount of data and cloud solutions seem attractive. However, there is fierce debate about the security of cloud datasets and the risk of their being compromised. Cloud solutions available on the market claim to be extremely resilient; however, the main concern is the trust that needs to be built between operators and cloud services providers. In certain cases, this trust has been established and even classified datasets are stored in the cloud.

The large amount of available data may be helpful in supporting decision making; however, advanced computational algorithms are required in order to harness this power. Artificial intelligence (AI) is an area that is expected to grow in the near future, to support decision making during a crisis but also to optimise critical infrastructure services during normal operations.

Finally, most critical infrastructures are expected in the long run to have some level of autonomy linked to AI. The sector that is expected to be revolutionised is transport. Autonomous cars are close to entering into production; they will change completely the way we move and travel, and the capacity of the existing network is expected to increase. Consequently, the management of transport infrastructure is going to change as a result of autonomous vehicles.

2.2.5 Stakeholders

2.2.5.1 European Union stakeholders

European Reference Network for Critical Infrastructure Protection

The mission of ERNCIP is to foster the emergence of innovative, qualified, efficient and competitive security solutions, through networking of EU experimental capabilities. It aims to link laboratories and facilities in order to carry out critical infrastructure-related security experiments and test new technology. It also contributes to improving the conditions for EU-wide certification and standardisation of security solutions.

The ERNCIP Office, run by JRC, is responsible for the management, coordination and administration of the ERNCIP project, under the supervision of Member State representatives and the Commission.

ERNCIP publishes annually a handbook to assist in the dissemination of the results of the network's activities. The latest edition was released in May 2018 (Gattinesi, 2018).

<https://erncip-project.jrc.ec.europa.eu/>

Critical Infrastructure Preparedness and Resilience Research Network

CIPRNet was funded as an FP7 security project, which started in March 2013 and finished in March 2017. CIPRNet created and maintains CIPedia, an online glossary of multinational definitions related to critical infrastructure protection. In addition, CIPRNet offered critical infrastructure protection training activities in the form of lectures and masterclasses.

To continue the work achieved within the project, 2EISAC was founded as a European non-profit association under German law focusing on critical infrastructure protection and resilience activities throughout Europe. Members are from EU Member States and associated states. The ultimate goal of 2EISAC is the foundation by 2020 of a distributed European infrastructure simulation and analysis centre.

www.ciprnet.eu

Critical Infrastructure Warning Information Network

The setting up of CIWIN⁽³²⁾ was one of the measures proposed in Commission communication COM(2006) 786 on EPCIP to facilitate the implementation of the programme. It has been operational since January 2013.

The network has two functions. First, it is an electronic forum for the exchange of information on critical infrastructure protection. Second, it is a rapid alert system for the delivery of early warnings from Member States to the Commission in relation to acute risks and threats to all. All Member States have signed a memorandum of understanding providing that they will contribute to the operation of this network.

DG Migration and Home Affairs coordinates all activities related to CIWIN.

https://ec.europa.eu/home-affairs/what-we-do/networks/critical_infrastructure_warning_information_network_en

Thematic Network on Critical Energy Infrastructure Protection

This network is made up of European owners and operators of energy infrastructures in the electricity, gas and oil sectors. It allows them to exchange information on threat assessment, risk management, cybersecurity and other related topics.

The network is an initiative of the Directorate-General for Energy.

<https://ec.europa.eu/energy/en/topics/infrastructure>

European Commission Directorate-General for Migration and Home Affairs

DG Migration and Home Affairs manages policies that aim to ensure that all activities necessary and beneficial to the economic, cultural and social growth of the EU can develop in a stable, lawful and secure environment. It aims to develop a balanced and comprehensive EU migration policy, based on solidarity and

⁽³²⁾ European Commission, 'Proposal for a Council Decision on a Critical Infrastructure Warning Information Network (CIWIN)' (COM(2008) 676 final), Brussels, 27.10.2008.

responsibility, building a safer Europe by fighting terrorism and organised crime, by promoting police cooperation and by preparing to respond swiftly to emerging crises.

DG Migration and Home Affairs is in charge of managing two dedicated EU funds: the Asylum, Migration and Integration Fund (AMIF) and the Internal Security Fund (ISF). The latter provides support for police cooperation, crime prevention and the fight against serious cross-border crime, including terrorism and violent extremism, as well as for crisis management and the protection of ECI (European Commission, 2016a).

https://ec.europa.eu/home-affairs/what-we-do/policies/crisis-and-terrorism/critical-infrastructure_en

European Commission Directorate-General for Energy

This DG is responsible for the EU's energy policy, with the aim of ensuring secure, sustainable and competitively priced energy for Europe.

In this context, DG Energy is engaged in the protection of the EU's critical energy infrastructure from disruption and damage.

<https://ec.europa.eu/energy/en/topics/infrastructure>

European Commission Directorate-General for Internal Market, Industry, Entrepreneurship and Small and Medium-sized Enterprises (SMEs)

DG Internal Market, Industry, Entrepreneurship and SMEs is the Commission department responsible for EU policy on the single market, industry, entrepreneurship and small businesses.

It is one of the Commission's actors engaged in building resilience by addressing potential strategic and critical sectors such as cybersecurity, critical infrastructures (energy, transport, space), the financial system, and public health (European Commission, 2016b).

https://ec.europa.eu/info/departments/internal-market-industry-entrepreneurship-and-smes_en#responsibilities

European Commission Directorate-General for International Cooperation and Development

This DG is responsible for EU policy on development and delivering international aid. It is in charge of international development cooperation, and it adapts to the evolving needs of partner countries, working closely with DG Neighbourhood and Enlargement Negotiations and other Commission services.

In the DG's strategic plan 2016-2020, specific objective 12 is as follows: 'Under the broader coverage of the legal bases of the Instrument contributing to Stability and Peace (IcSP) and the Instrument for Nuclear Safety Cooperation (INSC), [DG International Cooperation and Development] will address nuclear safety issues (EURATOM based) as well as specific global, trans-regional and emerging security threats, including among others chemical, biological, radiological and nuclear (CBRN) risks, terrorism and protection of critical infrastructure in third countries (TFEU based)' (European Commission, 2016c).

The IcSP addresses specific global and trans-regional threats to peace, international security and stability. It has three components: two implemented by the Service for Foreign Policy Instruments (activities linked to crisis management and peace building) and a third implemented by DG International Cooperation and Development (activities associated with global and trans-regional threats and emerging threats). This last component covers counterterrorism, CBRN risk mitigation, the fight against organised crime, protection of critical infrastructures, climate change and security.

https://ec.europa.eu/info/departments/international-cooperation-and-development_en#responsibilities

European Commission Directorate-General for Mobility and Transport

DG Mobility and Transport is responsible for EU policy in this area. It is engaged in aviation, maritime and land transport security. Among other tasks, and faced with the persistent threat of terrorism, it aims to reduce the vulnerability of public spaces related to transport infrastructures and to ensure a coordinated response in the event of a security incident on land, especially relating to rail travel (European Commission, 2016d).

https://ec.europa.eu/info/topics/transport_en

European Commission Directorate-General for Maritime Affairs and Fisheries

DG Maritime Affairs and Fisheries is responsible for EU policy on maritime affairs and fisheries. The action plan of the EUMSS for the global maritime domain, adopted in June 2014, is organised around five areas, the fourth being 'Risk management, protection of critical infrastructures and crisis response'; Section 4.3 covers assessing the resilience of maritime transport infrastructure to man-made and natural disasters and climate change (Council of the European Union, 2014a).

https://ec.europa.eu/info/departments/maritime-affairs-and-fisheries_en

European Commission Directorate-General Joint Research Centre

The JRC is the European Commission's science and knowledge service. It has solid research and policy support experience, developed in house, as well as broad networks with academia, industry, Member States and local authorities.

For more detailed information, see Section 3.4.

<https://ec.europa.eu/jrc/en/research-topic/critical-infrastructure-protection>

European Defence Agency

The EDA was established under a joint action of the Council of Ministers on 12 July 2004, 'to support the Member States and the Council in their effort to improve European defence capabilities in the field of crisis management and to sustain the European Security and Defence Policy as it stands now and develops in the future' ⁽³³⁾.

In October 2015, the EDA and the Commission jointly launched the Consultation Forum for Sustainable Energy in the Defence and Security Sector. Protection of critical energy infrastructures (PCEI) was identified as one of the areas to be examined and a PCEI expert group was set up. The work of the expert group is led by the ministries of defence of Cyprus and Greece, supported by their respective national academic communities and research centres. DG Energy and the JRC, as well as the NATO Energy Security Centre of Excellence (CoE), also support the work of the PCEI expert group, which explores options for protecting defence-related critical energy infrastructures from existing and emerging risks and threats, including hybrid and asymmetrical warfare, climate change and natural hazards (EDA, 2017a,b).

<https://www.eda.europa.eu>

European Union Agency for Cybersecurity (ENISA)

ENISA is a centre of expertise for cybersecurity in Europe. Since it was set up in 2004, it has actively contributed to a high level of network and information security (NIS) within the EU, to the development of a culture of NIS in society and to raising awareness of NIS, thus contributing to the proper functioning of the internal market. ENISA assists EU Member States in implementing relevant EU legislation and works to improve the resilience of Europe's critical information infrastructure and networks. Objective 1.1 of the ENISA programming document 2018-2020 relates to improving expertise related to critical information infrastructure (ENISA, 2017).

<https://www.enisa.europa.eu/>

European Global Navigation Satellite Systems Agency (GSA)

The GSA's core mission is to ensure that EU citizens get the most out of Europe's satellite navigation programmes, ensuring that European services and operations are thoroughly secure, safe and accessible. The GSA is positioning the Galileo Open Service as the answer to the demand for more and better synchronisation, on which many critical infrastructures, the telecom sector and financial services rely. The 5th issue of the *GNSS Market Report* states that the European global navigation satellite systems (GNSS) bring resilience to critical infrastructure. In particular, Galileo provides clear benefits to critical infrastructure operators thanks to its increasingly robust defences against spoofing and an increased number of satellites facilitating integrity monitoring and ensuring improved availability. GNSS are also used to monitor critical infrastructure and the natural environment to prevent major disaster and promptly intervene in case of emergency (GSA, 2017).

<https://www.gsa.europa.eu/>

⁽³³⁾ EDA, 'Mission' (<https://www.eda.europa.eu/Aboutus/Missionandfunctions>).

European Union Satellite Centre (SatCen)

According to its mission statement, 'the EU Satellite Centre supports the decision making and actions of the European Union in the field of Common Foreign and Security Policy (CFSP), in particular Common Security and Defence Policy (CSDP), including European Union crisis management missions and operations, by providing products and services resulting from the exploitation of relevant space assets and collateral data, including satellite imagery and aerial imagery, and related services' ⁽³⁴⁾. SatCen provides fast and reliable analyses of satellite data to meet current security challenges. In the field of critical infrastructure, it has been participating in studies on vulnerability assessment (i.e. evaluation of the likelihood of occurrence for various identified threats) based on spatially enabled data.

<https://www.satcen.europa.eu/>

2.2.5.2 International stakeholders

North Atlantic Treaty Organization

Significant research activity in the domain of defence-related critical infrastructures has been fostered by NATO's seven baseline requirements for resilience. NATO is currently working on supporting its member countries in identifying critical infrastructure dependencies and providing the tools to improve their resilience. Considering that military operations rely on critical infrastructures that are in principle operated by the private sector, it is not surprising that there are significant efforts to enhance civil-military collaboration.

https://www.nato.int/cps/en/natohq/news_161675.htm?selectedLocale=en

2.2.6 Legislation and reference documents

- European Commission, 'Green Paper on a European programme for critical infrastructure protection' (COM(2005) 576 final), Brussels, 17 November 2005.
- European Commission, Commission communication, 'European programme for critical infrastructure protection' (COM(2006) 786 final), Brussels, 12 December 2006.
- European Commission, 'Proposal for a Council Decision on a Critical Infrastructure Warning Information Network (CIWIN)' (COM(2008) 676 final), Brussels, 27 October 2008.
- Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection, OJ L 345, 23.12.2008, p. 75-82.
- European Commission, Commission staff working document, 'Review of the European programme for critical infrastructure protection (EPCIP)', SWD(2012) 190 final, Brussels, 22 June 2012.
- European Commission, Commission staff working document, 'A new approach to the European programme for critical infrastructure protection: making European critical infrastructures more secure' (SWD(2013) 318 final), Brussels, 28 August 2013.
- European Commission, Commission communication, 'The European agenda on security' (COM(2015) 185 final), Strasbourg, 28 April 2015.
- European Commission and High Representative of the Union for Foreign Affairs and Security Policy, joint communication, 'Joint framework on countering hybrid threats: a European Union response' (JOIN(2016) 18 final), Brussels, 6 April 2016.
- European Commission Communication, 'Delivering on the European agenda on security to fight against terrorism and pave the way towards an effective and genuine security union' (COM(2016) 230 final), Brussels, 20 April 2016.
- Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, OJ L 194, 19.7.2016, p. 1-30.

⁽³⁴⁾ SatCen, 'Mission, users and partners' (<https://www.satcen.europa.eu/who-we-are/our-mission>); see also Council Decision 2014/401/CFSP of 26 June 2014 on the European Union Satellite Centre and repealing Joint Action 2001/555/CFSP on the establishment of a European Union Satellite Centre, OJ L 188, 27.6.2014, p. 73-84.

- European Commission and High Representative of the Union for Foreign Affairs and Security Policy, joint communication, 'Resilience, deterrence and defence: building strong cybersecurity for the EU' (JOIN(2017) 450 final), Brussels, 13 September 2017.
- European Commission and High Representative of the Union for Foreign Affairs and Security Policy Joint Communication JOIN(2018) 16 final, Increasing resilience and bolstering capabilities to address hybrid threats, Brussels, 13 June 2018.

2.3 Public spaces protection

2.3.1 What are soft targets / public spaces?

There are two expressions used in this context: 'soft targets' and 'public spaces'. Although they are used to describe very similar things, the former is used more in relation to defence, while the latter is mainly used in a purely civilian context. Several English dictionaries define 'soft target'. For instance, according to the *Oxford English Dictionary*, it is 'A person or thing that is relatively unprotected or vulnerable, especially to military or terrorist attack' ⁽³⁵⁾, whereas in the *Cambridge Dictionary* a 'soft target' is defined as 'Something that is easy to attack or get an advantage from' ⁽³⁶⁾. *Collins Dictionary* defines it as 'A thing or a person that is easy to criticize or make an attack upon' ⁽³⁷⁾, and according to the online Free Dictionary 'soft target' is 'A military term referring to unarmoured/undefended non-military target' ⁽³⁸⁾.

Therefore, the phrases 'soft target' and 'public space' can refer, by definition, to a great variety of entities in terms of nature or type and size, from a single person to a city, the unifying characteristic — their softness — lying in the fact that they are in normal circumstances (relatively) unprotected or undefended, making them highly vulnerable to criminals or terrorists. Security practitioners and specialists tend for their part to use the term in the plural, 'soft targets', referring to places and areas that the general public, or certain parts of it, can access freely, combining a (high) concentration of people and a low degree of security against assault, thus making them relatively easy targets for terrorists. And this is clearly the definition of 'public spaces'. In this sense, they are usually opposed to 'hard targets', which are, on the contrary, highly secured premises and areas (e.g. military zones, some government and official buildings, and certain specific industrial infrastructures). In this report, we will use the expression 'public spaces', since this is the wording most commonly used in the EU.

Because of their open nature, a high concentration of people and the inherent low degree of security against assault, public spaces are also vulnerable to low-cost methods of attack. A ramming vehicle, home-made bomb or toy drone carrying explosives, to give but a few grim examples, are all cheap means by which not only to cause a number of fatalities but also to instil panic and fear, injuring European life, values and institutions at their very core.

Collective public spaces are numerous as shown by the following (non-exhaustive) list:

- places of study — schools, universities, libraries;
- public administration offices and public services;
- religious sites and places of worship;
- shopping centres and other commercial facilities;
- cultural venues — cinemas, theatres, concert halls, museums, galleries;
- bars, clubs, nightclubs, restaurants and hotels;
- hospitals and healthcare facilities;
- sporting arenas, sporting events and stadiums;
- railway stations, bus stations, ferry terminals and airports;
- parks, squares, beaches, tourist sites and places of interest;

⁽³⁵⁾ https://en.oxforddictionaries.com/definition/soft_target

⁽³⁶⁾ <https://dictionary.cambridge.org/fr/dictionnaire/anglais/soft-target>

⁽³⁷⁾ <https://www.collinsdictionary.com/dictionary/english/soft-target>

⁽³⁸⁾ <https://medical-dictionary.thefreedictionary.com/soft+target>

- fairs and marketplaces;
- parades, demonstrations, public meetings, pilgrimages and festivals;
- important transport sites.

2.3.2 Protecting public spaces

The increased number of attacks on public spaces since the beginning of 2000 and in particular during the past decade (see **Table 1**) demonstrates the need to increase security in public places. As stated by Kalvach et al. (2016), 'placing the soft targets [public spaces] in focus alongside the hard targets reflects an innovative attitude towards security management. We pay greater attention to the attackers' point of view and study the likelihood of an attack rather than its impact and social consequences'. This leads to '[providing] security to subjects which would traditionally not have been entitled to protection — commercial facilities, community events, private individuals etc.'.

However, public spaces are so numerous and different — despite their common intrinsic vulnerability due to their (more or less) open nature and public character — that it is almost impossible to provide security for all of them.

Indeed, as stated by John Cohen, a former counterterrorism coordinator for the US Department of Homeland Security, 'They are places that are difficult to harden because that would undermine the very reason they exist' (Keneally and Madden, 2017). He made this point after the mass shooting that killed 58 people and injured 851 others at an outdoor concert in Las Vegas in October 2017. He argued that eliminating the public's vulnerability in public spaces isn't necessarily possible, noting that officials tend to encourage people to go about their lives as normal after an attack.

This attitude is understandable, as it aims to counter the fear and anxiety that terrorists try to instil in people when carrying out their devastating acts, in addition to directly causing casualties and physical damage.

Despite the difficulties, many actions can be undertaken to reduce as much as possible the vulnerabilities of these public spaces, to detect threats at an earlier stage and to increase resilience at all levels.

2.3.3 The European Union scene and beyond

In the EU, which has been heavily impacted by terrorist attacks in recent years, the protection of public spaces has been high on the agenda, reflecting the great complexity of the task (in particular because of the heterogeneity of the potential targets, which range from fully open spaces to areas with some form of protection) and the many challenges that it poses for law enforcement, public health authorities and civil protection authorities, not only technically but also in finding the right balance between protection and people's individual and collective fundamental rights⁽³⁹⁾. According to the Council conclusions on the development of a renewed EU internal security strategy, 'respecting fundamental rights in planning and implementing internal security policies and action has to be seen as a means of ensuring proportionality, and as a tool for gaining citizens' trust and participation'⁽⁴⁰⁾.

The recent comprehensive assessment of EU security policy underlined the need to engage in 'a comprehensive approach to support soft target protection which could include aspects such as a risk assessment methodology, insider threats and vetting procedures, detection capacity, raising public awareness and training citizens, engaging with private stakeholders and harnessing new technology, in particular on detection and security by design'⁽⁴¹⁾.

Therefore, and although there is no EU legal instrument dealing with public space protection — a domain that falls primarily within Member States' responsibilities — the Commission has been active in the field. The EU action plan to support the protection of public spaces⁽⁴²⁾, issued in October 2017, outlines all the actions to be taken by the Commission. It highlights in particular new funding schemes, the fostering of exchange of best practices and public-private cooperation.

⁽³⁹⁾ Council of the European Union, Council conclusions on development of a renewed European Union internal security strategy, Brussels, 4 December 2014; European Commission communication COM(2015) 185 final.

⁽⁴⁰⁾ Council of the European Union, Council conclusions on development of a renewed European Union internal security strategy (2014).

⁽⁴¹⁾ European Commission, Commission staff working document, 'Comprehensive assessment of EU security policy' (SWD(2017) 278 final), Brussels, 26.7.2017.

⁽⁴²⁾ European Commission, Commission communication, 'Action plan to support the protection of public spaces' (COM(2017) 612 final), Brussels, 18.10.2017.

The Commission also created a forum to enhance cooperation and coordination between Member States, the EU Policy Group on Public Space Protection. A first EU workshop on public space protection, gathering experts from various disciplines, took place on 6-7 February 2017; a number of policy strands and actions were agreed among Member States. The Practitioners' Forum was also set up to facilitate exchange of information and expertise and the sharing of best practices on operational action to protect soft targets. It is intended mainly for Member State law enforcement practitioners and law enforcement networks. This has been complemented further by a newly established High Risk Security Network, which aims to bring together representatives of specialised law enforcement units responsible for the protection of high-risk public spaces. Through this network, a cross-border exercise, supported by the Commission and involving special intervention forces from the Belgian and Dutch police, took place on 29 June 2017, to test different approaches to soft target protection. The exercise consisted of a simulation of synchronised attacks on schools, aiming to measure preparedness and crisis management functions in case of simultaneous attacks in neighbouring countries ⁽⁴³⁾.

The EU Policy Group on Public Space Protection has also steered the work through a second stream, which has led to the creation of the Operators' Forum, which aims to engage with private operators and other relevant security stakeholders from the private sector (e.g. shopping malls, concert halls, car rental companies, etc.). The idea is to create a common awareness of current security challenges and encourage public-private security partnerships to improve protection.

One important aspect of the EU's work to protect public spaces is providing support to local authorities. City centres are very vulnerable owing to the large numbers of people gathering there. In March 2018, the EU mayors' conference organised by the Commission and the Committee of the Regions demonstrated the importance of sharing experiences among local authorities ⁽⁴⁴⁾. The JRC also organised in June 2018 a technical workshop on protecting city centres against terrorist attacks, to foster the exchange of practical information among urban planners and local security authorities (Karlos and Larcher, 2018). This work will be continued under the EU urban agenda, with a new partnership on security in public spaces.

Several funding schemes have also been adapted to reflect the increased need to protect public spaces. The Urban Innovative Fund aims to provide urban areas throughout Europe with resources to test new and unproven solutions to address urban challenges. The 2018 call included a budget for urban security ⁽⁴⁵⁾. The Internal Security Fund — Police promotes the implementation of the internal security strategy and law enforcement cooperation ⁽⁴⁶⁾. The new call seeks proposals in the field of public space protection, similar to the security projects carried out under H2020 ⁽⁴⁷⁾.

There are many other relevant initiatives at EU level and beyond, the international level being of prime importance in relation, for instance, to air transport infrastructures. One example is the EU aviation security framework, which has been developed over the years and is being constantly monitored, revised and reinforced in an attempt to stay ahead of the threat ⁽⁴⁸⁾.

With regard to the transport sector as a target ⁽⁴⁹⁾, whereas air transport is now significantly better protected, rail transport remains at high risk of attacks because of its open nature. On 15 June 2017, the Commission, with the Member States, launched a common railway risk assessment and is working on further measures to improve passenger railway security. The Commission has also been working on a best practice security guidance toolkit for the commercial road transport sector, which was published in January 2018. It provides operational guidance to help European truck drivers, haulage companies and other stakeholders to address cargo theft, stowaway entry to trucks and possible threats from terrorism. It also updates and upgrades

⁽⁴³⁾ European Commission, Commission communication, 'Ninth progress report towards an effective and genuine security union' (COM(2017) 407 final), Brussels, 26.7.2017; European Commission, Commission communication, 'Tenth progress report towards an effective and genuine security union' (COM(2017) 466 final), Brussels, 7.9.2017.

⁽⁴⁴⁾ European Commission, Commission communication, 'Thirteenth progress report towards an effective and genuine security union' (COM(2018) 46 final), Brussels, 24.1.2018.

⁽⁴⁵⁾ <https://www.uia-initiative.eu/en/call-proposals/4th-call-proposals>

⁽⁴⁶⁾ <http://ec.europa.eu/research/participants/portal/desktop/en/opportunities/isfp/topics/isfp-2018-ag-ct-protect.html>

⁽⁴⁷⁾ <http://ec.europa.eu/research/participants/portal/desktop/en/opportunities/h2020/topics/su-infra02-2019.html>

⁽⁴⁸⁾ The framework was built on efforts in collaboration with the United Nations: Regulation (EC) No 2320/2002 of the European Parliament and of the Council of 16 December 2002 establishing common rules in the field of civil aviation security, OJ L 355, 30.12.2002, p. 1-21; Regulation (EC) No 300/2008 of the European Parliament and of the Council of 11 March 2008 on common rules in the field of civil aviation security and repealing Regulation (EC) No 2320/2002, OJ L 97, 9.4.2008, p. 72-84; and subsequent revisions. The EU remains exposed to vulnerabilities in non-EU countries, in particular those facing a high level of terrorism threat and with lower aviation security standards.

⁽⁴⁹⁾ This sector presents the particularity that means of transport can also be used to conduct attacks (as in vehicle ramming).

contemporary good security practices that are rapidly becoming outdated amid constantly evolving threats, emerging technologies and regulatory changes ⁽⁵⁰⁾.

Maritime transport security is also under the scrutiny of the Commission, in particular to increase protection for maritime transport infrastructures (ports and port facilities) and ships (for container and passenger transport) ⁽⁵¹⁾.

More of these initiatives are described in Sections 2.3.5 and 2.3.6. They all contribute to supporting Member States at national, regional and local levels in their efforts to increase the protection of public spaces against future terrorist attacks and to increase overall resilience.

2.3.4 Possible evolution within the next 5 years

Attacks on public spaces could be of a terrorist nature, linked to a demonstration of ideological conviction, the result of emotional instability not linked to an ideology or a recurring pattern, or part of a more complex attack scenario (e.g. an element of hybrid warfare). By definition, the spectrum of public space vulnerability is broad and the methods of attack are diverse.

Relatively simple, low-cost methods such as vehicle ramming or shooting a firearm at a crowded space have been used to create casualties, fear and damage, and there is no reason to believe that such methods will not be used again in the future. As terrorist organisations are continually trying to innovate in terms of their techniques and *modi operandi*, more sophisticated assault techniques can be expected, such as the use of drones (sometimes referred to as ‘unmanned aerial systems’ or ‘unmanned aerial vehicles’ (UAVs)) carrying explosives or other harmful substances or weapons; drones have already been employed by Islamic State in Iraq and Syria (ISIS).

All transport systems are still a focus for terrorist groups. This concerns in particular air traffic, even though access to these systems is heavily controlled; the attractiveness of a successful attack remains high. In addition, rail transport is notably vulnerable. Access to transport hubs such as stations is very difficult to control, and therefore it is difficult to minimise the risk. Furthermore, the tracks themselves represent a critical target for operations such as derailing.

Risk analysis must also consider other potential methods of attack, which may presently appear highly improbable but which are becoming cheaper and more accessible through new technologies and thus more realisable.

Table 1: Non-exhaustive list of assaults against various types of public spaces in Europe in recent years, indicating the *modus operandi* (MO)

Schools
— Žďár nad Sázavou, Czechia, 2014; 1 fatality; MO: hostages, knife attack
— Toulouse, France, 2012; Jewish school; 4 fatalities and 1 injured; MO: shooting
Religious sites and places of worship
— Copenhagen, Denmark, 2015; outside a synagogue; 1 fatality and 2 injured; MO: shooting
— Brussels, Belgium, 2014; Jewish museum; 4 fatalities; MO: shooting
— Paris, France, 2015; kosher supermarket; 4 fatalities; MO: shooting, hostages
— Saint-Étienne-du-Rouvray, France, 2017; church; 1 fatality and 1 injured; MO: knife attack, hostages
Transport
— Belgium–France, 2015; Thalys train attack; 4 injured; MO: shooting

⁽⁵⁰⁾ European Commission, Commission communication, ‘Eleventh progress report towards an effective and genuine security union’ (COM(2017) 608 final), Brussels, 18.10.2017; European Commission communication COM(2018) 46 final.

⁽⁵¹⁾ Council of the European Union (2014a).

<ul style="list-style-type: none"> — Brussels, Belgium, 2016; Zaventem airport terminal; 16 fatalities and 100 injured; MO: suicide bombing — Brussels, Belgium, 2016; metro station; 16 fatalities and more than 200 injured; MO: suicide bombing — Würzburg, Germany, 2016; train attack; 5 injured; MO: attack with hatchet and knife
Cultural and sports venues/events
<ul style="list-style-type: none"> — Paris, France, 2015; football match; 1 fatality; MO: suicide bombing — Paris, France, 2015; concert hall; 129 fatalities and 354 injured; MO: shooting — Copenhagen, Denmark, 2015; cultural centre; 1 fatality and 3 injured; MO: shooting
Shopping centres and restaurants
<ul style="list-style-type: none"> — Paris, France, 2015; restaurant terraces; 39 fatalities and 32 injured; MO: shooting from a car — Copenhagen, Denmark, 2015; 1 fatality; MO: shooting — Carcassonne and Trèbes, France, 2018; car and supermarket; 4 fatalities and 15 injured; MO: shooting, hostages
City centres
<ul style="list-style-type: none"> — Dijon, France, 2014; city centre; 13 injured; MO: car driving into a crowd — Nice, France, 2016; Promenade des Anglais; 86 fatalities and 458 injured; MO: truck driving into a crowd — Berlin, Germany, 2016; Christmas market; 12 fatalities and 56 injured; MO: truck driving into a crowd — Stockholm, Sweden, 2017; city centre; 5 fatalities and 14 injured; MO: van driving into a crowd — Manchester, United Kingdom, 2017; Manchester Arena foyer; 22 fatalities and 512 injured; MO: suicide bombing — Barcelona, Spain, 2017; city centre; 15 fatalities and 180 injured; MO: car driving into a crowd — Cambrils, Spain, 2017; city centre; 1 fatality and several injured; MO: car driving into a crowd — Paris, France, 2017; Avenue des Champs-Élysées; 1 fatality and 3 injured; MO: shooting — London, United Kingdom, 2017; Westminster area; 5 fatalities and 44 injured; MO: car driving into a crowd, knife attack
Others
<ul style="list-style-type: none"> — Paris, France, 2015; headquarters of the newspaper Charlie Hebdo; 12 fatalities and 12 injured; MO: shooting

Note: Not all attacks listed are necessarily only terrorism-related.

Source: Authors.

2.3.5 Stakeholders

2.3.5.1 European Union stakeholders

EU Policy Group on Public Space Protection

The EU Policy Group on Public Space Protection was launched in February 2017. As described in the action plan to support the protection of public spaces ⁽⁵²⁾, its aim is to improve cooperation and coordination between Member States, to bring together national policymakers and to collect, exchange and disseminate best practices. The group will advise the Commission on actions on the protection of public spaces and will steer the work through two streams: the Practitioners' Forum and the Operators' Forum.

⁽⁵²⁾ European Commission communication COM(2017) 612 final.

The former connects law enforcement practitioners and networks to enable them to exchange expert knowledge on the protection of public spaces. The Operators' Forum involves private entities operating public spaces, such as shopping malls or concert halls, and other relevant private stakeholders, with the aim of improving security awareness and encouraging public-private security partnerships to improve protection. The first meeting of the Operators' Forum took place in December 2017, and focused on information exchange and guidance on detection, as well as on the testing of new technology and security solutions ⁽⁵³⁾.

European Commission Directorate-General for Migration and Home Affairs

DG Migration and Home Affairs manages policies that aim to ensure that all activities necessary and beneficial to the economic, cultural and social growth of the EU can develop in a stable, lawful and secure environment. It aims to develop a balanced and comprehensive EU migration policy, based on solidarity and responsibility, building a safer Europe by fighting terrorism and organised crime, by promoting police cooperation and by preparing to respond swiftly to emerging crises. As stated in its 2018 management plan, DG Migration and Home Affairs supports the implementation of the action plan on protecting public spaces (European Commission, 2018).

https://ec.europa.eu/home-affairs/index_en

European Commission Directorate-General for Mobility and Transport

DG Mobility and Transport is responsible for EU policy in this area. It is engaged in aviation, maritime and land transport security. Among other tasks, and faced with the persistent threat of terrorism, it aims to reduce the vulnerability of public spaces related to transport infrastructures and to ensure a coordinated response in the event of a security incident on land, especially relating to rail travel (European Commission, 2016d).

https://ec.europa.eu/transport/themes/security_en

EU Airport Police Network (Airpol)

Airpol is an operational network of airport-related law enforcement agencies. Its mission is to enhance the overall security of EU airports and the civil aviation domain by optimising the effectiveness and efficiency of airport- and aviation-related law enforcement and border guard activities, and by contributing to a more harmonised approach to enforcement in this area. In May 2014, the Commission and Airpol developed a manual on soft target protection at EU airports ⁽⁵⁴⁾.

<https://www.airpoleuropa.eu/>

European Network of Railway Police Forces (Railpol)

Railpol is an international network of organisations responsible for policing the railways in EU Member States. The aim is to enhance and intensify international railway police cooperation in Europe, to prevent threats and to guarantee the effectiveness of measures against cross-border crime. It operates through working groups on various subjects, including public order and counterterrorism. The main goals of these groups are to exchange best practices and share information, draw up recommendations, analyse reports and organise joint international days of action ⁽⁵⁵⁾.

<https://www.railpol.eu/site/home>

European Union Agency for Law Enforcement Cooperation (Europol)

Europol is the EU's law enforcement agency, and its mission is to support EU Member States in preventing and combating all forms of serious international organised crime and terrorism. Its European Counter Terrorism Centre (ECTC) is an operations centre and hub of expertise in the fight against terrorism, focusing on, for example, providing operational support for investigations to EU Member States, international cooperation among counterterrorism authorities and tackling foreign fighters.

<https://www.europol.europa.eu/>

⁽⁵³⁾ European Commission, 'Security union: Commission follows up on terrorist radicalisation' (https://ec.europa.eu/commission/presscorner/detail/en/IP_18_381).

⁽⁵⁴⁾ European Commission, 'Implementation of the European agenda on security: questions and answers' (https://ec.europa.eu/commission/presscorner/detail/en/MEMO_16_2594).

⁽⁵⁵⁾ Railpol annual review 2017.

European Commission Directorate-General for Regional and Urban Policy

DG Regional and Urban Policy manages policies aimed at reducing disparities in development between the various EU regions. As part of its activities, it contributes to the Commission priority of migration, mainly through measures financed under the European Regional Development Fund, such as Urban Innovative Actions. The aim of these actions is to create a space in which cities throughout Europe feel free to experiment with potential solutions to the challenges they face (European Commission, 2016e).

https://ec.europa.eu/info/departments/regional-and-urban-policy_en

European Committee of the Regions

The Committee of the Regions is the EU's assembly of regional and local representatives. Together with the European Commission, the committee organised a conference in Brussels on 8 March 2018, which brought together mayors from a large number of European cities, including those cities that had been hit by terrorist attacks, in order to facilitate an exchange on the protection of public spaces, draw lessons from recent attacks and identify best practices emerging in cities across the Union ⁽⁵⁶⁾. The Committee of the Regions has drafted recommendations for an action plan to support the protection of public spaces, drawn up by the Commission ⁽⁵⁷⁾.

<https://cor.europa.eu/en>

European Commission Directorate-General Joint Research Centre

The JRC is the European Commission's science and knowledge service. It has solid research and policy support experience, developed in house, as well as broad networks with academia, industry, Member States and city authorities.

The JRC provides scientifically based evidence supporting the policies in the field of public space protection of DG Migration and Home Affairs, EEAS (through the EU Intelligence and Situation Centre), DG Mobility and Transport and DG Regional and Urban Policy. It is actively involved in the implementation of the action plan on protecting public spaces. For more detailed information, see Section 3.4.

https://ec.europa.eu/info/departments/joint-research-centre_en

2.3.6 Legislation and reference documents

- European Commission, Commission communication, 'Action plan to enhance preparedness against chemical, biological, radiological and nuclear security risks' (COM(2017) 610 final), Brussels, 18 October 2017.
- European Commission, Commission communication, 'Action plan to support the protection of public spaces' (COM(2017) 612 final), Brussels, 18 October 2017.

2.4 Critical supplies security

2.4.1 What are critical supplies?

Critical supplies can be defined as those supplies vital to the support of operations that, owing to various causes, are or are expected to be in short supply ⁽⁵⁸⁾.

In this report, the notion is applied to non-fuel/non-food raw materials as well as to energy fuel supply. There is growing concern within the EU and beyond regarding the increasing use and high supply risk of a number of raw materials and fuels, putting the EU economy at risk of supply shortages. Securing non-energy and energy supply chains is therefore a key priority for the EU's economic and social life.

More generally, the question of availability and access to natural resources is at stake. In a recent study, the World Economic Forum states: 'The availability of natural resources, particularly food, water, energy and minerals, is an important issue but also a highly contested one, mostly because of the many different

⁽⁵⁶⁾ European Commission communication COM(2018) 46 final.

⁽⁵⁷⁾ European Committee of the Regions, 'Tackling terrorism: local leaders welcome EU plans to invest in cities to protect communities' (<http://cor.europa.eu/en/news/Pages/Tackling-terrorism-local-leaders-welcome-EU-plans-to-invest-in-cities-to-protect-communities0308-2981.aspx>).

⁽⁵⁸⁾ <https://www.thefreedictionary.com/critical+supplies+and+materiel>

perspectives and opinions held by both experts and the general public' (World Economic Forum, 2014, p. 3). The report proposes a new paradigm that 'shows that while the world has sufficient global stocks of natural resources to meet most of society's demands, the flow of resource distribution is increasingly threatened by highly uncertain "above ground" factors. Similarly local crises risk having disproportionate global effects on resources, due to the high level of interconnections among resources and the factors influencing their availability. This, in turn, indicates a need for heightened care in addressing social and environmental considerations' (World Economic Forum, 2014, p. 5).

This explains the global context in which the situation described hereafter with regard to the security of raw materials and fuel supplies in the EU is embedded.

2.4.2 Securing the supply of raw materials and fuels in the European Union

Raw materials (including non-fuel and non-food ones) and energy fuels will be considered successively in subsection.

2.4.2.1 Non-fuel and non-food raw materials

The European raw materials initiative and the notion of critical raw material

Non-fuel and non-food materials such as metals, minerals and forest-based materials have become increasingly important to the EU's economy, as they constitute crucial inputs into a wide range of high-value goods and applications in a number of industrial sectors, such as automotives, aerospace, steel, electronics and renewable energy, to name only a few.

However, because of an increased global competition for access to a sustainable supply of many of these raw materials, the EU may end up sometimes in a severe situation because of its low level of self-sufficiency and high level of consumption of products that are rich in various raw materials. The severity is expressed as supply risk, reflecting the risk of a disruption in the EU supply of the materials. Weak links in critical supply chains may further threaten the transition towards clean technologies and also have a negative impact on defence capabilities, health services, food production and distribution systems and transport systems. Considering complete and shifting supply chains is therefore essential when assessing the security of supply of raw materials.

As a consequence, the European Commission adopted in 2008 the European raw materials initiative ⁽⁵⁹⁾, as part of which it proposed a number of measures aimed at:

- securing a fair and sustainable supply of raw materials from international markets;
- fostering sustainable supply within the EU;
- boosting resource efficiency and promoting recycling.

One of the main actions under the initiative was the introduction of the concept of a critical raw material in which the methodology for assessing criticality is based on economic importance and supply risk. This resulted in an initial list of 14 critical non-energy raw materials ⁽⁶⁰⁾. The list was accompanied by the following information, illustrating the concept of critical raw materials: 'The 14 raw materials listed are critical because the risks of supply shortage and their impacts on the economy are higher compared with most of the other raw materials. Their high supply risk is mainly due to the fact that a high share of the worldwide production mainly comes from a handful of countries: China, Russia, the Democratic Republic of Congo and Brazil (niobium and tantalum). This concentration of production is in many cases compounded by low substitutability and low recycling rates.'

The original list was to be updated at least every 3 years; therefore, two revised lists have been published, in 2014, with 20 critical raw materials ⁽⁶¹⁾, and in 2017, with 27 critical raw materials ⁽⁶²⁾.

⁽⁵⁹⁾ European Commission, Commission communication, 'The raw materials initiative — meeting our critical needs for growth and jobs in Europe' (COM(2008) 699 final), Brussels, 4.11.2008.

⁽⁶⁰⁾ European Commission, Commission communication, 'Tackling the challenges in commodity markets and on raw materials' (COM(2011) 25 final), Brussels, 2.2.2011.

⁽⁶¹⁾ European Commission, Commission communication, 'Review of the list of critical raw materials for the EU and the implementation of the raw materials initiative' (COM(2014) 297 final), Brussels, 26.5.2014; this followed European Commission, Commission report, *Implementation of the Raw Materials Initiative* (COM(2013) 442 final), Brussels, 24.6.2013.

⁽⁶²⁾ European Commission, Commission communication, '2017 list of critical raw materials for the EU' (COM(2017) 490 final), Brussels, 13.9.2017; European Commission (2017a).

The list contributes to implementing EU industrial policy, aiming in particular to (European Commission, 2017a):

- strengthen the competitiveness of EU industry in line with the renewed industrial strategy for Europe ⁽⁶³⁾;
- stimulate the production of critical raw materials by enhancing new mining and recycling activities in the EU;
- foster efficient use and recycling of critical raw materials;
- increase awareness of potential raw material supply risks and related opportunities among EU countries, companies and investors;
- provide support to innovation on raw material supply under the H2020 research and innovation programme;
- support the negotiation of trade agreements, challenge trade distortion measures, develop research and innovation actions and implement the 2030 Agenda for Sustainable Development and the Sustainable Development Goals.

Other EU actions related to the raw material initiative

Several other policies contributing to the implementation of the Europe 2020 strategy relate to the supply of raw materials needed for EU industry ⁽⁶⁴⁾, including the following.

- The European innovation partnership (EIP) on raw materials, targeting non-energy, non-agricultural raw materials, supports innovation and jobs by creating a multistakeholder platform to guide EU policy in this area ⁽⁶⁵⁾. In several documents released by the EIP, specific actions and orientations are mentioned.
 - The Commission will, within the framework of the EU Raw Materials Strategy, identify bottlenecks and supply risks linked to the materials that are necessary for the development of key capabilities ... Future EU research programmes could also be used to mitigate supply risks, including substitution of critical raw materials, building on the work in the area of Key Enabling Technologies (KETs) ⁽⁶⁶⁾.
 - The Commission has developed the concept of 'hybrid standards' for dual-use products to support security-related research. In implementing the Communication on cybersecurity, the Commission, in cooperation with Member States and industry, is developing a European certification framework and exploring a voluntary labelling framework for the security of ICT products, products that are dependent on the supply of around 16 EU-declared critical raw materials.
- The eco-innovation action plan, which is part of the Innovation Union flagship initiative, focuses on specific bottlenecks, challenges and opportunities for achieving environmental objectives through innovation ⁽⁶⁷⁾.
- The EU action plan for the circular economy, as part of the circular economy package ⁽⁶⁸⁾ under the responsibility of the Commission's Secretariat-General, was adopted at the end of 2015 to support the circular economy in each step of the whole value chain, from production to consumption, repair and manufacturing, waste management and secondary raw materials that are fed back into the economy ⁽⁶⁹⁾.

⁽⁶³⁾ European Commission, Commission communication, 'Investing in a smart, innovative and sustainable industry: a renewed EU industrial policy strategy' (COM(2017) 479 final), Brussels, 13.9.2017.

⁽⁶⁴⁾ See, for example, European Commission, Commission communication, 'Roadmap to a resource efficient Europe' (COM(2011) 571 final), Brussels, 20.9.2011; European Commission, Commission communication, 'For a European industrial renaissance' (COM(2014) 14 final), Brussels, 22.1.2014.

⁽⁶⁵⁾ European Commission, 'European innovation partnership (EIP) on raw materials' (<https://ec.europa.eu/growth/tools-databases/eip-raw-materials/>).

⁽⁶⁶⁾ According to the European Commission, "KETs are a group of six technologies: micro and nanoelectronics, nanotechnology, industrial biotechnology, advanced materials, photonics, and advanced manufacturing technologies. They have applications in multiple industries and help tackle societal challenges"; https://ec.europa.eu/growth/industry/policy/key-enabling-technologies_en; consulted on 19 September 2018.

⁽⁶⁷⁾ European Commission, Commission communication, 'Innovation for a sustainable future — the eco-innovation action plan (Eco-AP)' (COM(2011) 899 final), Brussels, 15.12.2011.

⁽⁶⁸⁾ European Commission, 'Circular economy' (http://ec.europa.eu/environment/circular-economy/index_en.htm).

⁽⁶⁹⁾ European Commission, Commission communication, 'Closing the loop — an EU action plan for the circular economy' (COM(2015) 614 final), Brussels, 2.12.2015.

However, it is very important to be aware that sustainable raw material usage and recycling cannot cover current and future EU needs for such materials, and that securing the primary raw material supply from outside the EU will also be necessary. The Commission's circular economy principles — new technological solutions and business models with more sustainable production, consumption and waste management — should also be applied to the defence sector, in which resource efficiency and security of supplies are increasingly important.

2.4.2.2 Energy fuels

The EU currently imports 54 % of its energy fuels (90 % of its crude oil, 69 % of its natural gas, 42 % of its coal and other solid fuels, and 40 % of its uranium and other nuclear fuels), with this sector accounting for more than 20 % of total EU imports ⁽⁷⁰⁾.

The energy mix is also shifting notably, moving towards more renewable sources, leading to the use of, for instance, more wind turbines, solar panels and ocean energy. These new technologies and plants (e.g. photovoltaic farms) rely on various raw materials to function, largely imported from non-EU countries, which implies, as for the 'old technologies', the need to have secure access to these materials.

The supply of fuels to the EU, which is of vital importance, is exposed to various types of risks, externally and internally, ranging from problems and disruptions in exporting countries to terrorist attacks and hybrid threats, not forgetting extreme weather events. Therefore, to increase the security of energy supply and the resilience of the EU's energy system, an EU energy security strategy was launched in 2014 ⁽⁷¹⁾, addressing long-term challenges to the security of supplies through five main issues, which are described below in a quotation from the DG Energy website ⁽⁷²⁾:

- increasing energy efficiency, focusing on buildings and industry (accounting for 40 % and 25 % of total energy consumption respectively in the EU);
- reducing EU energy dependency on third countries and also diversifying supplier countries and routes;
- completing the internal energy market and building missing infrastructure links to respond quickly to supply disruptions and redirect energy across the EU to where it is needed;
- speaking with one EU voice in external energy policy, ensuring also that Member States inform the European Commission early on planned agreements with third countries that may affect the EU's security of supply;
- strengthening emergency and solidarity mechanisms and protecting critical infrastructure.

The main energy sectors are all covered by legislation or proposed legislation aimed at securing fuel supplies: the security of gas supply regulation ⁽⁷³⁾ (one quarter of all the energy used in the EU is natural gas, and many EU countries import nearly all their supplies), the minimum stocks of crude oil and/or petroleum products directive ⁽⁷⁴⁾ (Member States are required to maintain oil stocks equal to at least 90 days of their average daily consumption) and the Commission proposal for a new regulation on electricity risk-preparedness ⁽⁷⁵⁾ (to prevent and manage electricity blackouts).

These precautionary actions are of the greatest importance, as any disruption in fuel supply or malfunctioning of the fuel supply chain would affect all sectors of society, and in particular the defence capabilities of the EU and its Member States.

⁽⁷⁰⁾ European Commission, 'Energy security' (<https://ec.europa.eu/energy/en/topics/imports-and-secure-supplies>).

⁽⁷¹⁾ European Commission, Commission communication, 'European energy security strategy' (COM(2014) 330 final), Brussels, 28.5.2014.

⁽⁷²⁾ European Commission, 'Energy security strategy' (<https://ec.europa.eu/energy/en/topics/energy-strategy-and-energy-union/energy-security-strategy>).

⁽⁷³⁾ Regulation (EU) 2017/1938 of the European Parliament and of the Council of 25 October 2017 concerning measures to safeguard the security of gas supply and repealing Regulation (EU) No 994/2010, OJ L 280, 28.10.2017, p. 1-56.

⁽⁷⁴⁾ Council Directive 2009/119/EC of 14 September 2009 imposing an obligation on Member States to maintain minimum stocks of crude oil and/or petroleum products, OJ L 265, 9.10.2009, p. 9-23.

⁽⁷⁵⁾ European Commission, 'Proposal for a Regulation of the European Parliament and the Council on risk-preparedness in the electricity sector and repealing Directive 2005/89/EC' (COM(2016) 862 final), Brussels, 27.10.2008.

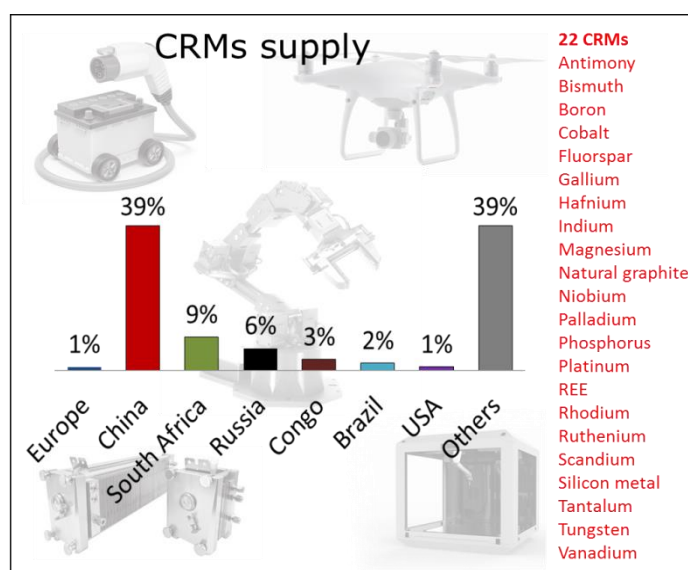
2.4.2.3 The case of the defence sector

Defence is a sector that is highly sensitive to the availability of non-fuel and fuel raw materials and therefore requires the highest possible level of supply security. Consequently, the European defence action plan ⁽⁷⁶⁾ of 2016 contains a full section on strengthening security of supply, forming the first of the three pillars of the action plan ('Reinforcing the single market for defence').

According to this section, 'The Commission will, within the framework of the EU Raw Materials Strategy, identify bottlenecks and supply risks linked to the materials that are necessary for the development of key capabilities building on the findings of a recent study [Pavel and Tzimas, 2016]. Future EU research programmes could also be used to mitigate supply risks, including substitution of critical raw materials, building on the work in the area of Key Enabling Technologies (KETs).'

Several dual-use technologies — namely advanced batteries and fuel cells, unmanned systems, robotics and 3D printing technology — have been thoroughly examined and assessed in view of demand for materials and security of supply issues ⁽⁷⁷⁾. Europe's dependence on the supply of raw materials is extremely high. Europe produces around 3 % of the raw materials required for these technologies, whereas China dominates global production, supplying one third of all the raw materials needed for the technologies in question. Other key suppliers are South Africa, Russia, Brazil, Australia and Chile. With regard to the supply of critical raw materials, Europe provides only 1 % of them. The major supplier is China, with an almost 40 % share, followed by South Africa and Russia (**Figure 1**). The main raw material risks across batteries, fuel cells, robotics and drones relate to supplies of cobalt, natural graphite and silicon metal, for which the major suppliers are the Democratic Republic of Congo and China. Vanadium and magnesium are also high risk, given their use in several dual-use technologies.

Figure 1: Key suppliers of critical raw materials (CRMs) for advanced Lithium-ion batteries, fuel cells, robotics, drones and 3D printing



Source: JRC internal report to DG Internal Market, Industry, Entrepreneurship and SMEs (2019).

2.4.2.4 The trade and diplomacy perspective

Raw materials play a significant role in EU trade policy, which must ensure that global markets operate in a free and transparent way. Many non-EU countries, however, apply measures such as export taxes, import duties or price-fixing to raw materials, which distorts markets and could be detrimental to the EU's manufacturing industries. Consequently, the EU's implements its trade strategy along three lines:

1. defining the 'rules of the game' through bilateral and multilateral negotiations;

⁽⁷⁶⁾ European Commission communication COM(2016) 950 final.

⁽⁷⁷⁾ JRC internal report to DG Internal Market, Industry, Entrepreneurship and SMEs, *Materials dependencies for dual-use technologies relevant for Europe's defence sector* (2019).

2. enforcing the rules and tackling market barriers when required;
3. promoting debate on raw materials, both in bilateral and in multilateral settings.

As part of its raw materials strategy, the EU pursues raw materials diplomacy and is engaged in a number of bilateral and multilateral dialogues and strategic partnerships. So far, the EU has developed relations with Argentina, Brazil, Canada, Chile, China, Colombia, Greenland, Japan, Mexico, Peru, the United States, Uruguay, the EuroMed countries and the African Union ⁽⁷⁸⁾.

There is also an EU energy diplomacy strategy in place ⁽⁷⁹⁾, involving close cooperation between the EEAS and the European Commission, and resulting from the Commission communication on a resilient energy union (February 2015), the European Council conclusions recognising the importance of the external dimension of the Energy Union (March 2015) and the Foreign Affairs Council adopting Council conclusions on EU energy diplomacy, which include an EU energy diplomacy action plan (July 2015) ⁽⁸⁰⁾.

2.4.3 Possible evolution within the next 5 years

The following trends are anticipated:

- serious threats are not expected in the next 5 years;
- price increases and imbalances between supply and demand for some metals are possible;
- a new rare earths crisis is improbable in the short term;
- mitigation measures (e.g. increasing efficiency, substitution and recycling) will continue to be developed;
- attention should be paid to supplies of critical materials, in particular those associated with high and increasing demand, such as cobalt, lithium (in batteries), rare earths (in wind turbines and electric vehicles), composite materials, etc.

2.4.4 Stakeholders

2.4.4.1 European Union stakeholders

European Commission Directorate-General for Internal Market, Industry, Entrepreneurship and SMEs

DG Internal Market, Industry, Entrepreneurship and SMEs is responsible for EU policy on the single market, industry, entrepreneurship and small businesses.

One of its many tasks is ensuring a secure, sustainable and affordable supply of raw materials (European Commission, 2016b). DG Internal Market, Industry, Entrepreneurship and SMEs is in particular responsible for the EIP on raw materials and for the European Rare Earth Competency Network.

https://ec.europa.eu/growth/sectors/raw-materials_en

European Commission Directorate-General for Energy

DG Energy is responsible for developing a resilient energy union with a forward-looking climate policy, in order to ensure affordable, secure and sustainable energy for businesses and households alike.

One of its objectives is to contribute to the security of energy supply, based on solidarity and trust (European Commission, 2016f).

<https://ec.europa.eu/energy/en/topics/imports-and-secure-supplies>

European Commission Directorate-General for Environment

This DG is responsible for EU policy on the environment. It proposes and implements policies that ensure a high level of environmental protection and preserve the quality of life of EU citizens.

⁽⁷⁸⁾ European Commission, 'Raw materials diplomacy' (https://ec.europa.eu/growth/sectors/raw-materials/specific-interest/international-aspects_en).

⁽⁷⁹⁾ EEAS, 'EU energy diplomacy' (https://eeas.europa.eu/topics/energy-diplomacy/406/eu-energy-diplomacy_en).

⁽⁸⁰⁾ European Commission, Commission communication, 'A framework strategy for a resilient energy union with a forward-looking climate change policy' (COM(2015) 80 final), Brussels, 25.2.2015; Council of the European Union, Council conclusions EUCO 11/15, Brussels, 20.3.2015; Council of the European Union, Council conclusions on energy diplomacy (10995/15), Brussels, 20.7.2015.

It is responsible for the implementation of the circular economy action plan (European Commission, 2016g) (specific objective 1 includes ensuring that the EU economy is resource-efficient, green and competitive).

http://ec.europa.eu/environment/circular-economy/index_en.htm

European Commission Directorate-General for Trade

This DG is responsible for EU policy on trade with countries beyond the EU's borders. This includes raw materials (European Commission, 2016h).

<http://ec.europa.eu/trade/policy/accessing-markets/goods-and-services/raw-materials/>

European Commission Directorate-General Joint Research Centre

The JRC is the European Commission's science and knowledge service. It has solid research and policy support experience, developed in house, as well as broad networks with academia, industry, Member States and city authorities.

For more information about research in the area of critical supplies, see Section 3.4.

https://ec.europa.eu/info/departments/joint-research-centre_en

European Institute of Innovation and Technology (EIT)

The EIT is an independent EU body. It aims to enhance Europe's ability to innovate by nurturing entrepreneurial talent and supporting new ideas.

EIT RawMaterials was designated an EIT Innovation Community by the EIT Governing Board on 9 December 2014.

<https://eit.europa.eu/eit-community/eit-raw-materials> and <https://eitrawmaterials.eu/>

European Defence Agency

The EDA was established under a joint action of the Council of Ministers on 12 July 2004, 'to support the Member States and the Council in their effort to improve European defence capabilities in the field of crisis management and to sustain the European Security and Defence Policy as it stands now and develops in the future'.

The EDA works to ensure an adequate level of confidence in security of supply across Europe, including long-term assurance of sources of key technologies and willingness of partner governments to facilitate supply. The EDA's work is based on a pragmatic step-by-step approach, reaching a common understanding on and taking into account the different aspects of security of supply.

In addition, its energy and environment programme aims, among its objectives, to 'reduce [the dependency of European military forces] on imported fossil fuels, improve energy efficiency, integrate new energy technologies into military capabilities and to understand the cultural and management issues that exist within the military that restrict overall sustainability and resilience'.

<https://www.eda.europa.eu> and <https://www.eda.europa.eu/what-we-do/activities/activities-search/energy-and-environment-programme>

Agency for the Cooperation of Energy Regulators (ACER)

The EU agency ACER was created as part of the third energy package to further progress the completion of the internal energy market both for electricity and for natural gas.

ACER contributes to achieving the EU's energy policy objectives, including an efficient energy infrastructure guaranteeing the free movement of energy across borders and the transportation of new energy sources, thus enhancing security of supply for EU businesses and consumers.

https://www.acer.europa.eu/en/The_agency/Pages/default.aspx

Euratom Supply Agency (ESA)

The Euratom Supply Agency was established by the Art 52 of the Euratom Treaty to ensure a regular and equitable supply of nuclear fuels to EU users in line with the objectives of Art 2(d). ESA also implements the EU common supply policy for nuclear materials and monitors transactions involving services in the nuclear fuel cycle (conversion, enrichment and fuel fabrication).

The remit of the agency was strengthened in 2008 by the Council Decision, establishing ESA's statutes which entrusted the agency with the creation of a nuclear market observatory.

<https://ec.europa.eu/euratom/index.html>

2.4.4.2 International stakeholders

Organisation for Economic Co-operation and Development (OECD)

The European Commission supports the work of the OECD on raw materials. This work concentrates on the raw materials trade, tackling export restrictions, promoting best practices in raw material policies and due diligence for responsible supply chains. The OECD provides economic analysis of trade in the sector and a forum for multilateral discussions.

<http://www.oecd.org/tad/benefitlib/export-restrictions-raw-materials.htm>

United Nations

Among the 17 Sustainable Development Goals of the 2030 Agenda for Sustainable Development adopted by the UN in 2015 in order 'to promote prosperity while protecting the planet', Goal 12 aims at 'ensuring sustainable consumption and production patterns. Sustainable consumption and production is about promoting resource and energy efficiency, sustainable infrastructure, and providing access to basic services, green and decent jobs and a better quality of life for all.' This goal is further specified in a series of 11 targets, such as 'Implement the 10-year framework of programmes on sustainable consumption and production, all countries taking action, with developed countries taking the lead, taking into account the development and capabilities of developing countries' and 'By 2030, achieve the sustainable management and efficient use of natural resources'.

<https://www.un.org/sustainabledevelopment/sustainable-consumption-production/>

North Atlantic Treaty Organization

Regarding energy security, NATO performs regular consultations among allies and partner countries, shares intelligence sharing and expands links with relevant international organisations, such as the International Energy Agency and the EU. NATO also organises the North Atlantic Council's annual seminars on global energy developments, as well as the Energy Security Strategic Awareness Course, which has taken place annually since 2015. NATO supports national authorities in enhancing their resilience to energy supply disruptions that could affect national and collective defence.

https://www.nato.int/cps/en/natohq/topics_49208.htm

2.4.5 Legislation and reference documents

- European Commission, Commission communication, 'The raw materials initiative — meeting our critical needs for growth and jobs in Europe' (COM(2008) 699 final), Brussels, 4 November 2008.
- Council of Directive 2009/119/EC of 14 September 2009 imposing an obligation on Member States to maintain minimum stocks of crude oil and/or petroleum products, OJ L 265, 9.10.2009, p. 9-23.
- European Commission, Commission communication, 'Tackling the challenges in commodity markets and on raw materials' (COM(2011) 25 final), Brussels, 2 February 2011.
- European Commission, Commission report, *Implementation of the raw materials initiative* (COM(2013) 442 final), Brussels, 24 June 2013.
- European Commission, Commission communication, 'Review of the list of critical raw materials for the EU and the implementation of the raw materials initiative' COM(2014) 297 final, Brussels, 26 May 2014.
- European Commission, Commission communication, 'European energy security strategy' (COM(2014) 330 final), Brussels, 28 May 2014.
- European Commission, Commission staff working document, 'In-depth study of European energy security' (SWD(2014) 330 final), accompanying COM(2014) 330 final, Brussels, 2 July 2014.
- European Commission, *Report on Critical Raw Materials for the EU: Report of the Ad Hoc Working Group on Defining Critical Raw Materials*, May 2014.

- European Commission, Commission communication, 'A framework strategy for a resilient energy union with a forward-looking climate change policy' (COM(2015) 80 final), Brussels, 25 February 2015.
- Council of the European Union, Council conclusions EUCO 11/15, Brussels, 20 March 2015.
- Council of the European Union, Council conclusions on energy diplomacy (10995/15), Brussels, 20 July 2015.
- European Commission, Commission communication, 'European defence action plan' (COM(2016) 950 final), Brussels, 30 November 2016.
- European Commission, 'Proposal for a Regulation of the European Parliament and the Council on risk-preparedness in the electricity sector and repealing Directive 2005/89/EC' (COM(2016) 862 final), Brussels, 30 November 2016.
- European Commission, Commission communication, '2017 list of critical raw materials for the EU' (COM(2017) 490 final), Brussels, 13 September 2017.
- Regulation (EU) 2017/1938 of the European Parliament and of the Council of 25 October 2017 concerning measures to safeguard the security of gas supply and repealing Regulation (EU) No 994/2010, Strasbourg, OJ L 280, 28.10.2017, p. 1-56.

2.5 Cybersecurity

2.5.1 What are cyber-threats?

Terrorist groups and some political or ideological extremist groups have found in the internet an effective way to promote, plan, support and execute acts of terrorism or hate crimes with the help of hacktivists or transnational criminal organisations.

From a defence perspective, an increasing number of nations have found ways of using the internet as a multifaceted weapon. The boundaries of conflicts become uncertain; attack scenarios are never declared, making difficult to identify who is performing the attack, hence, making even harder to take the proper defence countermeasures. Cybersecurity concerns almost everyone, from individuals to business communities and states, while issues committing the states to counter political, ideological extremist groups and state-sponsored hackers are predominantly cyber defence related.

The ongoing technological evolution has led to a new form of conflict targeting critical societal functions, government digital services, and economic and financial development. Strategically, targeted actions in cyberspace could be designed either to inflict physical damage or to provoke emotional and psychological effects, inducing fear or mistrust in society as a result of service disruptions or by taking control of digital data information systems and networks.

The internet, the web, computer systems, mobile devices, all kinds of data and social networking — in a single word cyberspace — is the battlefield for approximately four billion global internet users, half of the world population. In addition, a large part of this environment, the deep web, needs to be investigated.

According to International Standard ISO/IEC 27032:2012 ⁽⁸¹⁾:

- cybersecurity is defined as 'preservation of confidentiality, integrity and availability of information in the cyberspace';
- cyberspace is the 'complex environment resulting from the interaction of people, software and services on the Internet by means of technology devices and networks connected to it, which do not exist in any physical form'.

Cyberattacks on public and private infrastructure are currently considered an aspect of the hybrid threats that the EU will have to face and challenge (see Section 2.7). Cyberspace is the specific context for the analysis of the various potential threats as a result of which a strategic shift is taking place from cybersecurity activities to cyberdefence-related actions. Although a clear definition of the concept is lacking (Dewar, 2017), the notion of 'active cyberdefence' is increasingly being used by relevant actors. Researcher Robert S. Dewar of the Geneva Centre for Security Policy defines it as 'a concept predicated upon deploying tools to not only identify and stop cyber incidents as they are occurring, but also taking offensive measures

⁽⁸¹⁾ International Organisation for Standardisation, 'ISO/IEC 27032:2012' (<https://www.iso.org/standard/44375.html>).

to minimize attackers' capabilities. This can be achieved through a variety of technical solutions such as deploying decoys or hacking the attackers' own networks to neutralize their efforts' (Dewar, 2017).

Therefore, the intention in this section is to avoid referring simply and directly to cybersecurity as such, addressing more specifically cyberdefence, which relates closely to the topic of hybrid threats. A new hybrid model of cybersecurity defence and response is rapidly emerging and possible cyberattacks against EU public/private infrastructure data and systems have established the need for a different approach in the use of IT assets and networks. This is currently being effected through a series of actions and negotiations both at EU and at international levels, including the engagement of scientists for the development of responsible and innovative counterattack measures.

2.5.2 How do 'state hackers' or 'hacktivists' operate?

Hackers are systems and computer security experts able to break into computer networks to steal, change, destroy information or tamper with digital devices. Hacktivists are hackers who are politically or socially motivated and intend to strategically jeopardise vital societal services and systems. The frequency of cyberattacks against local, national and foreign governments and their critical infrastructures continues to grow; these results could provoke physical damage leading to conventional hostilities. Attacks could affect or shut down power grids, cause oil pipelines to explode, contaminate water supplies, cause the collision of aeroplanes or disrupt military or intelligence satellites. Not only systems or structures but also data and information are very attractive to nation state hackers, and not merely for financial gain. As recently reported (Brattberg and Maurer, 2018), extracted or stolen data have been used to influence voting in some elections.

2.5.3 Reform of cybersecurity in the European Union

Cybersecurity is an essential element of the EU digital single market strategy ⁽⁸²⁾. The EU has introduced a set of legislative measures, a public-private partnership, a certification scheme and a cybersecurity competence network, as well as reinforcing the role of the EU cybersecurity agency. Developing a cyberdefence policy and capabilities under the CSDP is part of the EU's cybersecurity plan to protect the open internet and online freedom and opportunity.

2.5.3.1 Cybersecurity Strategy of the European Union

Since 2013, with the adoption of an EU cybersecurity strategy ⁽⁸³⁾ setting out the vision, roles, responsibilities and required actions in the domain of cybersecurity, the EU has proposed many initiatives and measures that focus on and/or include cybersecurity, privacy and cybercrime aspects. In the context of developing a cyberdefence policy, the HR/VP has called for a focus on:

- assessing operational EU cyberdefence requirements;
- developing the EU cyberdefence policy framework;
- improving cyberdefence training and exercise opportunities for the military;
- promoting dialogue and coordination between civilian and military actors in the EU;
- ensuring dialogue with international partners, including NATO.

The strategy specifies roles and responsibilities both at national and EU levels for three key pillars — NIS, law enforcement and defence — involving dialogue on policy with international partners, such as the Council of Europe, the OECD, the Organization for Security and Co-operation in Europe (OSCE), NATO and the UN.

In addition, the strategy states that the forthcoming arrangements for the implementation of the Solidarity Clause (Article 222 of the Treaty on the Functioning of the European Union (TFEU)) should take into consideration the risk of cyberattack against a Member State.

⁽⁸²⁾ European Commission, 'Digital single market' (<https://ec.europa.eu/digital-single-market/en>).

⁽⁸³⁾ European Commission and High Representative of the Union for Foreign Affairs and Security Policy, joint communication, 'Cybersecurity strategy of the European Union: an open, safe and secure cyberspace' (JOIN (2013) 1 final), Brussels, 7.2.2013.

2.5.3.2 Strengthening Europe's cyber-resilience system and fostering a competitive and innovative cybersecurity industry

This communication ⁽⁸⁴⁾ aims to strengthen Europe's cyber-resilience system and foster a competitive and innovative cybersecurity industry in Europe, so that Europe is prepared to face a possible large-scale cyber-crisis that could affect critical information systems in several Member States simultaneously. For this purpose, cyber-aspects should be integrated into existing crisis management mechanisms, and information sharing and cooperation among Member States should be effective.

Cooperation is envisaged in the directive on security of network and information systems, the NIS directive ⁽⁸⁵⁾, of 2016, for example through the Computer Security Incident Response Team (CSIRT) network (which promotes effective operational cooperation on specific cybersecurity incidents and sharing of information about risks) and the Cooperation Group (which supports strategic cooperation and exchange of information related to cyber-incidents among Member States). To reinforce further the implementation of the directive, the Commission proposed additional measures in a communication of 2017 ⁽⁸⁶⁾.

To address intersectoral interdependencies and key public network infrastructure resilience, the Commission recommended various actions in its communication. These included facilitating cooperation among sectoral Information Sharing and Analysis Centres ⁽⁸⁷⁾ and CSIRTs, studying the strategic/systemic risk resulting from cyber-incidents in highly interdependent sectors, setting up trusted channels for voluntary reporting on cyber-theft of trade secrets and promoting the embedding of cybersecurity measures in European sectoral policies.

To stimulate the competitiveness and innovation of Europe's cybersecurity industry, the Commission signed with industry a contractual public-private partnership on cybersecurity in July 2016 ⁽⁸⁸⁾, launched H2020 calls for proposals related to the cybersecurity partnership and ensured coordination of the cybersecurity partnership through relevant sectoral strategies, H2020 instruments and sectoral public-private partnerships.

2.5.3.3 Resilience, deterrence and defence

To better protect Europe against cyberattacks, the Commission and the HR/VP proposed in September 2017 a wide-ranging set of measures to build strong cybersecurity in the EU.

The joint communication ⁽⁸⁹⁾ describes a package of measures building on existing instruments and presenting new initiatives to further improve EU cyber-resilience and response in three key areas:

1. building EU resilience to cyberattacks and stepping up the EU's cybersecurity capacity;
2. creating an effective criminal law response;
3. strengthening global stability through international cooperation.

As part of the package of measures, the Commission presented a proposal for a regulation ⁽⁹⁰⁾, referred to as the Cybersecurity Act, to deal with cyberattacks and to build strong cybersecurity in the EU. The act reinforces the mandate of ENISA, to enable it to better support Member States in tackling cybersecurity threats and attacks, and it also establishes an EU framework for cybersecurity certification, boosting the cybersecurity of online services and consumer devices.

⁽⁸⁴⁾ European Commission, Commission communication, 'Strengthening Europe's cyber resilience system and fostering a competitive and innovative cybersecurity industry' (COM(2016) 410 final), Brussels, 5.7.2016.

⁽⁸⁵⁾ Directive (EU) 2016/1148.

⁽⁸⁶⁾ European Commission, Commission communication 'Making the most of NIS — towards the effective implementation of Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union' (COM(2017) 476 final/2), Brussels, 4.10.2017.

⁽⁸⁷⁾ These centres are non-profit organisations that provide a central resource for gathering information on cyber-threats as well as allowing two-way sharing of information between the private and the public sector; see ENISA, 'Information Sharing and Analysis Centers (ISACs)' (<https://www.enisa.europa.eu/topics/national-cyber-security-strategies/information-sharing>).

⁽⁸⁸⁾ European Commission, 'Commission signs agreement with cybersecurity industry to increase measures to address cyber threats' (<https://ec.europa.eu/digital-single-market/en/news/commission-signs-agreement-cybersecurity-industry-increase-measures-address-cyber-threats>).

⁽⁸⁹⁾ European Commission and High Representative of the Union for Foreign Affairs and Security Policy, joint communication, 'Resilience, deterrence and defence: building strong cybersecurity for the EU' (JOIN(2017) 450 final), Brussels, 13.9.2017.

⁽⁹⁰⁾ European Commission, 'Proposal for a Regulation of the European Parliament and of the Council of the European Union on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification ("Cybersecurity Act")' (COM(2017) 477 final/2), Brussels, 4.10.2017.

More generally, to complete the EU digital single market, the package also includes:

- the swift implementation of the NIS directive;
- a cybersecurity certification scheme ⁽⁹¹⁾;
- the establishment of a blueprint for how to respond to large-scale cyberattacks;
- the launch of a European Cybersecurity Industrial, Technology and Research Competence Centre, with a network of similar centres at Member State level ⁽⁹²⁾;
- a more effective criminal law response to cybercrime through a new directive to fight fraud and counterfeiting of non-cash payments.

With regard to cyberdefence, the framework for a joint EU diplomatic response to malicious cyber-activities (the 'Cyber Diplomacy Toolbox') ⁽⁹³⁾ sets out the measures under the CFSP, including restrictive measures, that can be used to strengthen the EU's response to activities that harm its political, security and economic interests. Implementation work on the framework is currently ongoing with Member States and will be taken forward taking into account the blueprint ⁽⁹⁴⁾ for responding to large-scale cyber-incidents. More particularly, the EU aims to drive high-end skills development among civilian and military professionals by providing solutions to help with national efforts and by setting up a cyberdefence training and education platform.

The EU cybersecurity strategy also identifies developing cyberdefence policy and capabilities related to the framework of the CSDP as one of its objectives, and it outlines a list of actions envisaged to increase collaboration between the EDA and the Member States.

2.5.3.4 The European Union cyberdefence policy framework

The Council of the European Union conclusions on common security and defence policy of November and December 2013 ⁽⁹⁵⁾ called for the development of an EU cyberdefence policy framework, on the basis of a proposal by the HR/VP, in cooperation with the European Commission and the EDA.

The Council conclusions ⁽⁹⁶⁾ related to the joint communication of September 2017 recognised the need for a renewed emphasis on the implementation of the 2014 EU cyberdefence policy framework (Council of the European Union, 2014b) and to update it to further integrate cybersecurity and defence into the CSDP and into the wider security and defence agenda. Furthermore, they stressed the need to step up cooperation on cyberdefence and to take full advantage of the proposed defence initiatives to accelerate the development of adequate cyber-capabilities in Europe.

The cyberdefence policy framework called for increased civil-military cooperation and synergies with wider EU cyber policies, relevant EU institutions and agencies, and the private sector. Since its adoption, a number of objectives have been implemented and a list of priorities established. In December 2017, the Council published a report on the implementation of the cyberdefence policy framework (Council of the European Union, 2017a).

⁽⁹¹⁾ European Commission, 'The EU cybersecurity certification framework' (<https://ec.europa.eu/digital-single-market/en/eu-cybersecurity-certification-framework>).

⁽⁹²⁾ This has been further implemented by the adoption of European Commission, 'Proposal for a Regulation of the European Parliament and of the Council of the European Union establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres' (COM(2018) 630 final), Brussels, 12.9.2018.

⁽⁹³⁾ Council of the European Union, Council conclusions on a framework for a joint EU diplomatic response to malicious cyber activities ('Cyber Diplomacy Toolbox') (9916/17), Brussels, 7.6.2017.

⁽⁹⁴⁾ European Commission, Commission recommendation on coordinated response to large scale cybersecurity incidents and crises (C(2017) 6100 final), Brussels, 13 September 2017

⁽⁹⁵⁾ Council of the European Union, Council conclusions partly on common security and defence policy (EUCO 217/13), Brussels, 20.12.2013; Council of the European Union, Council conclusions on common security and defence policy (15992/13), Brussels, 25.11.2013.

⁽⁹⁶⁾ Council of the European Union, Council conclusions on the joint communication to the European Parliament and the Council: Resilience, deterrence and defence: Building strong cybersecurity for the EU (14435/17), Brussels, 20.11.2017.

Table 2: Timeline of implementation of the EU cyberdefence policy framework

Date	Document reference	Document description
March 2013	N/A	Cyberdefence capability requirements statement
19 December 2013	EUCO 217/13	Council of the European Union conclusions
7 February 2013	JOIN(2013) 1 final	EU cybersecurity strategy 2013
18 November 2014	15532/2/14 REV 2	Council conclusions on CSDP
18 November 2014	15585/14	EU cyberdefence policy framework
18 May 2015	8971/15	Council conclusions on CSDP
26 June 2015	10347/15	First report on the implementation of the cyberdefence policy framework
10 November 2015	13801/15	Second report on the implementation of the cyberdefence policy framework
February 2016	NA	Technical arrangement between the Computer Emergency Response Team of the EU and the NATO Computer Incident Response Capability
1 June 2016	9701/16	Third report on the implementation of the cyberdefence policy framework
8 July 2016	NA	Joint declaration by the President of the European Council, the President of the European Commission and the Secretary-General of
22 November 2016	EEAS(2016) 1597	EU concept for cyberdefence for EU-led military operations
25 November 2016	14904/16	Fourth report on the implementation of the cyberdefence policy framework
7 June 2017	9916/17	Council conclusions on a framework for a joint EU diplomatic response to malicious cyber activities ('Cyber Diplomacy Toolbox')
12 June 2017	EEAS(2017) 773	Concept for integrating cybersecurity into the planning and conduct of civilian CSDP missions
13 September 2017	JOIN(2017) 450 final	Joint communication, 'Resilience, deterrence and defence: building strong cybersecurity for the EU'
9 October 2017	13007/17	Implementing guidelines for the framework on a joint EU diplomatic response to malicious cyber activities
13 November 2017	14190/17	Council conclusions on security and defence in the context of the EU global strategy
20 November 2017	14435/17	Council conclusions on the joint communication on resilience, deterrence and defence
6 December 2017 5 December 2017	14802/17 15283/16	Council conclusions on the implementation of the EU-NATO joint declaration
19 December 2017	15870/17	Annual report on the implementation of the cyberdefence policy framework

Source: Authors.

To mention some examples, the EDA launched in 2017 a cooperative mechanism to encourage national cyberdefence exercises and training, involving 11 Member States. More broadly, the EU's defence ministers took part in EU Cybrid 2017, a table-top exercise on strategic-level responses to cyberattacks against EU missions. The purpose of the exercise, under the Estonian Presidency, was to raise awareness of the impact of cyberattacks on EU military structures and to provide training on the coordination of crisis response measures. Many cyber aspects have been included in EU and NATO exercise scenarios with the intention of enhancing cyberdefence cooperation. The EU and NATO have also agreed on exchanging information and sharing best practices between their respective emergency response teams, the Computer Emergency Response Team of the European Union (CERT-EU) and NATO's Computer Incident Response Capability.

2.5.3.5 The general data protection regulation and the directive on security of network and information systems

With the full entry into force of the NIS directive, a higher common level of security of network and information systems will be achieved within the EU, enhancing cybersecurity capabilities at national level and further cooperation on risk management, baseline security measures and incident reporting obligations for critical infrastructure operators of essential services and digital service providers. These measures, together with the general data protection regulation⁽⁹⁷⁾, will contribute to the legal basis that is indispensable in providing stability and improved security to the digital single market while ensuring fundamental freedoms and privacy protection. Furthermore, under the umbrella of the NIS, the legislator is starting to inject in sectorial policy cybersecurity elements, to implement a cybersecurity by design approach also in the policies. The Commission has just published a report with key findings on how the EU cybersecurity rules under the NIS Directive are implemented in the crucial energy sector, in particular in electricity, gas and oil areas⁽⁹⁸⁾. Other examples are related to the last policies in the sectors of transport, border management and radio equipment.

2.5.4 Possible evolution within the next 5 years

With full digitalisation, the vulnerability of our society to cyberattacks will certainly increase. Cybersecurity will increasingly become a matter of national security and as a direct consequence it is reasonable to expect cyber-conflicts to escalate in terms of frequency and magnitude, targeting not only traditional critical infrastructures but also other layers of digital society. Military forces as well as diplomacy will be required to enforce national security in a completely new, non-military dimension.

State-sponsored attacks may lead to the deployment of cyber-capabilities in a military context, although the attribution of a cyber-threat still remains very difficult. Research and innovation are needed to protect national interests from cyberattacks.

As cyberspace has been declared by the Council of the European Union to be a military domain — the fifth domain of operations, alongside land, sea, air and space — strategic autonomy in information technology is becoming increasingly important for civil and military infrastructures. Just as the battlefield is expanding in cyberspace, countermeasures in support of societal vital interests will have to be further developed. The deployment of AI techniques is expected to be a game-changer for next-generation cyberdefence.

The dual use component in ICT and cybersecurity will be key for preventing and reacting to these emerging cyber-risks. Increased civil-military cooperation should take place and new research on cyberdefence carried out, starting with an assessment of the incremental effect of combining the two dimensions. Needs in relation to developing a common approach should be identified, available tools and capabilities fully exploited, and common curricula and guidelines developed.

2.5.5 Stakeholders

2.5.5.1 European Union stakeholders

European Commission Directorate-General for Communications Networks, Content and Technology (Connect)

Connect is responsible for managing the digital agenda. The DG's efforts in cybersecurity are mainly channelled through the NIS directive and specific actions under the digital single market agenda (e.g. the contractual public-private partnership on cybersecurity, accompanying measures on security certification and labelling of ICT products and security, the NIS directive and the general data protection regulation). The European Commission, through Connect, and the HR/VP have proposed a wide range of specific measures that will further strengthen the EU's cybersecurity structures and capabilities through more cooperation.

https://ec.europa.eu/info/departments/communications-networks-content-and-technology_en

⁽⁹⁷⁾ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 4.5.2016, p. 1-88.

⁽⁹⁸⁾ NIS Cooperation Group (2019).

European Commission Directorate-General for Migration and Home Affairs

DG Migration and Home Affairs manages policies that aim to ensure that all activities necessary and beneficial to the economic, cultural and social growth of the EU can develop in a stable, lawful and secure environment. It aims in particular to build a safer Europe by fighting terrorism and organised crime, by promoting police cooperation and by preparing to respond swiftly to emerging crises. Promoting cybersecurity and fighting against cybercrime in the EU is one of its most important tasks (European Commission, 2016a).

https://ec.europa.eu/info/departments/migration-and-home-affairs_en#responsibilities

European Commission Directorate-General for Energy

DG Energy focuses on creating a competitive internal energy market to lower prices, develop renewable energy sources, and reduce energy dependence and energy consumption. Like other Commission services in charge of industrial or service sectors, DG Energy is responsible for specific actions addressing security, and by extension cybersecurity. For instance, in 2017 it organised, together with Connect, a high-level round table on the main challenges for cybersecurity in the energy system. The DG continued its work with expert groups, including stakeholder consultations to analyse vulnerabilities and cyber-risks in the energy system (European Commission, 2017b). For this purpose, a Smart Grids task force was set up in 2009 to advise on issues related to smart grid deployment and development. It consists of five expert groups which focus on specific areas. Their work shape EU smart grid policies and the policy framework. In April 2019, the Commission has adopted a Recommendation⁽⁹⁹⁾ that provides guidance on how to address the specific challenges of the energy sector on cybersecurity. It identifies the main actions required to preserve cybersecurity and be prepared to possible cyberattacks in the energy sector, taking into account the characteristics of the sector such as the real-time requirements, the risk of cascading effects, and the combination of legacy systems with new technologies.

https://ec.europa.eu/info/departments/energy_en#responsibilities

European Commission Directorate-General for Mobility and Transport

The aim of the Commission in terms of transport is to promote, through DG Mobility and Transport, a mobility that is efficient, safe, secure and environmentally friendly and to create the conditions for a competitive industry generating growth and jobs. One of the general objectives of the DG is to support the development and deployment of intelligent transport systems and the digitalisation of transport, as contributions to the emergence of a connected digital single market. This requires, in particular, that it address cybersecurity issues (European Commission, 2016d).

https://ec.europa.eu/info/departments/mobility-and-transport_en#responsibilities

European Commission Directorate-General Joint Research Centre

The JRC is the European Commission's science and knowledge service. It has solid research and policy support experience, developed in house, as well as broad networks with academia, industry, Member States and city authorities. The JRC is very active in the field of research and policy support for cybersecurity. See Section 3.4 for more details.

<https://ec.europa.eu/jrc/en/research-topic/cybersecurity>

European Union Agency for Cybersecurity (ENISA)

This agency, set up in 2004, works closely with the Member States and private sector to deliver advice and solutions. This includes, among other activities, the pan-European cybersecurity exercises, the development of national cybersecurity strategies, and CSIRT cooperation and capacity building, as well as studies on the cyberthreat landscape, secure cloud adoption, data protection issues, privacy-enhancing technologies, and privacy issues relating to emerging technologies, electronic identification and trust services. ENISA also supports the development and implementation of the EU's policy on matters related to the security of network and information systems.

In May 2018, the agency signed a memorandum of understanding to establish a cooperation framework between their organisation with the EDA, EC3 and CERT-EU. The framework aims to leverage synergies between the four organisations, promoting cooperation on cybersecurity and cyberdefence, and it is a

⁽⁹⁹⁾ European Commission, Commission Recommendation (EU) 2019/553 on cybersecurity in the energy sector (notified under document C(2019) 2400), Brussels, 3 April 2019.

testament to the trusted partnership that exists between these EU agencies. It focuses on five areas of cooperation: exchange of information, education and training, cyber-exercises, technical cooperation, and strategic and administrative matters ⁽¹⁰⁰⁾.

<https://www.enisa.europa.eu/>

Computer Emergency Response Team of the European Union

CERT-EU, established in September 2012, is the permanent computer emergency response centre for all EU institutions, agencies and bodies. It is made up of IT security experts from the main EU institutions (the European Commission, the Council, the European Parliament, the Committee of the Regions, and the Economic and Social Committee). It cooperates closely with CERTs in the Member States and beyond as well as with specialised IT security companies. Its mission is to support the EU institutions to help them protect themselves against intentional and malicious attacks that would hamper the integrity of their IT assets and harm the interests of the EU. The scope of CERT-EU's activities covers prevention, detection, response and recovery.

https://cert.europa.eu/cert/plainedition/en/cert_about.html

The European Network of Law Enforcement Technology Services (Enlets)

Enlets was established as a subgroup of the Law Enforcement Working Party of the Council of the European Union in 2008 during the French Presidency of the Council. The main goals of this subgroup are to strengthen police activities and cooperation and to promote the use of modern technologies in the process of exchanging information, knowledge or experiences. Within Enlets, the Mobile Identification Interoperability Group is a subgroup aimed at bringing together examples of good practice and advice for Member States in relation to developing and using mobile identification devices for police and immigration services.

https://ec.europa.eu/home-affairs/financing/fundings/projects/HOME_2012_ISEC_FP_C2_4000003994_en

European Data Protection Supervisor (EDPS)

The EDPS is the EU's independent data protection authority; it ensures that EU institutions and bodies respect people's right to privacy when processing their personal data. In particular, the EDPS (i) supervises the EU administration's processing of personal data to ensure compliance with privacy rules, (ii) advises EU institutions on all aspects of personal data processing and related policies and legislation, (iii) handles complaints and conducts inquiries, (iv) works with the national authorities of EU Member States to ensure consistency in data protection and (v) monitors new technologies that might have an impact on data protection.

https://edps.europa.eu/edps-homepage_en

European External Action Service

The EEAS is the EU's diplomatic service. A key aspect of the work of the EEAS is its ability to work closely with the foreign and defence ministries of the EU Member States and with EU institutions. It also has a strong working relationship with the UN and other international organisations. It helps the HR/VP to implement the EU's CFSP.

The EEAS, together with DG Migration and Home Affairs and DG Connect, implements the CSDP. They also co-authored the 2013 EU cybersecurity strategy ⁽¹⁰¹⁾.

https://eeas.europa.eu/headquarters/headquarters-homepage_en

⁽¹⁰⁰⁾ EDA, 'Four EU cybersecurity organisations enhance cooperation' (<https://www.eda.europa.eu/info-hub/press-centre/latest-news/2018/05/23/four-eu-cybersecurity-organisations-enhance-cooperation>).

⁽¹⁰¹⁾ See JOIN (2013) 1 final.

European Defence Agency

The EDA is an intergovernmental agency of the Council of the European Union, to which it reports and from which it receives guidelines. The Agency has three main missions: (1) supporting the development of defence capabilities and military cooperation among the EU Member States, (2) stimulating defence research and technology and strengthening the European defence industry and (3) acting as a military interface for EU policies.

One of the domains in which the EDA is active is cyber- and hybrid warfare. This work comprises several projects on topics such as: cyberdefence, communications and information systems and hybrid warfare.

<https://www.eda.europa.eu/what-we-do/activities/activities-search/cyber-defence>

European Union Agency for Law Enforcement Cooperation (Europol)

Europol is the EU's law enforcement agency; it supports the EU Member States in their fight against terrorism, cybercrime, and other serious and organised forms of crime. It also works with many non-EU partner states and international organisations.

The European Union Internet Referral Unit (EU IRU) was set up by the Justice and Home Affairs Council of the EU and is built upon Europol's Check-the-Web service. Its main role is to anticipate and pre-empt terrorist abuse of online tools, as well as to play a proactive advisory role in relation to EU Member States and the private sector in this regard.

The EUIRU is a key unit of Europol's ECTC and focuses on:

- supporting the competent EU authorities by providing strategic and operational analysis;
- flagging terrorist and violent extremist online content and sharing it with relevant partners;
- detecting and requesting the removal of internet content used by smuggling networks to attract migrants and refugees;
- swiftly carrying out and supporting the referral process, in close cooperation with the industry.

Besides the support provided to the EU Member States, EU IRU cooperates closely with third-party partners within the framework of the EU Internet Forum. In this context and with the European Commission's support, EU IRU has engaged with online service companies to promote self-regulation activities by the online industry. The EU Internet Forum is a platform launched by the European Commission on 3 December 2015, bringing together EU interior ministers, a number of internet companies, Europol and the EU Counter-Terrorism Coordinator. The aim of the forum has been to address, in a coordinated manner, the phenomenon of the spread of terrorist and violent extremist propaganda to a large proportion of the global online population.

<https://www.europol.europa.eu/about-europol/european-counter-terrorism-centre-ectc>

The European Cybercrime Centre

EC3 was set up by Europol in 2013 to strengthen law enforcement responses to cybercrime in the EU. EC3 contributes to the fight against cybercrime through a three-pillar approach: forensics, strategy and operations. It has been involved in high-profile operations and on-the-spot operational support deployments resulting in many arrests, and has analysed huge numbers of files, the vast majority of which have proven to be malicious.

EC3 produces annually the *Internet Organised Crime Threat Assessment*, which reports the key findings and emerging threats and developments in cybercrime.

<https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3>

2.5.5.2 International stakeholders

North Atlantic Treaty Organization

On 8 July 2016, a joint declaration on an EU–NATO partnership was signed by the President of the European Council, the President of the European Commission and the Secretary-General of NATO. It identifies seven areas of cooperation, one of which is cybersecurity and defence coordination in the context of missions and operations, exercises, and education and training. NATO and EU cyber-incident response teams regularly exchange policy updates and best practices on cyberdefence.

https://www.nato.int/cps/en/natohq/topics_78170.htm

Within NATO, the Cooperative Cyber Defence CoE is a multinational and interdisciplinary hub of cyberdefence expertise. The Tallinn-based international military organisation focuses on technology, strategy, operations and law. NATO CoE are nationally or multinationally funded institutions that train and educate leaders and specialists from NATO member and partner countries, assist in doctrine development, identify lessons learned, improve interoperability and capabilities, and test and validate concepts through experimentation.

<https://ccdcoe.org/>

United Nations International Telecommunication Union (ITU)

Based on the guidance of the World Summit on the Information Society, held in two phases in Geneva (2003) and Tunis (2005), and the ITU Plenipotentiary Conference, the role of ITU is to build confidence and security in the use of ICT. At the summit, heads of state and world leaders entrusted ITU to be the facilitator of Action Line C5, 'Building confidence and security in the use of ICTs', in response to which ITU launched, in 2007, the Global Cybersecurity Agenda as a framework for international cooperation in this area.

<https://www.itu.int/en>

European Telecommunications Standards Institute (ETSI)

ETSI, a European standards organisation set up in 1988, produces globally applicable standards for ICT, including fixed, mobile, radio, converged, broadcast and internet technologies. One of the ETSI technical committee deals with cybersecurity (TC Cyber), looking at standardisation of cybersecurity internationally and providing a centre of relevant expertise for other ETSI committees. TC Cyber focuses on the security of infrastructures, devices, services and protocols, as well as on security assurance tools and techniques. The committee works with stakeholders to develop appropriate standards to increase privacy and security for organisations and citizens across Europe. It offers security advice and guidance to users, manufacturers, and network and infrastructure operators. The standards it produces are freely available online.

<https://www.etsi.org/committee/1393-cyber>

2.5.6 Legislation and reference documents

- European Parliament Resolution 2013/2606(RSP) on a cybersecurity strategy of the European Union: an open, safe and secure cyberspace, Strasbourg, 12 September 2013.
- Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (eIDAS), OJ L 257, 28.8.2014, p. 73-114.
- Council of the European Union, *EU Cyber Defence Policy Framework* (15585/14), Brussels, 18 November 2014.
- European Commission, Commission communication, 'The European agenda on security' (COM(2015) 185 final), Strasbourg, 28 April 2015.
- European Commission, Commission communication, 'A digital single market strategy for Europe' (COM(2015) 192 final), Brussels, 6 May 2015.
- European Commission and High Representative of the Union for Foreign Affairs and Security Policy, joint communication, 'Joint framework on countering hybrid threats: a European Union response' (JOIN(2016) 18 final), Brussels, 6 April 2016.

- European Commission, Commission communication COM(2016) 230 final, 'Delivering on the European agenda on security to fight against terrorism and pave the way towards an effective and genuine security union', Brussels, 20 April 2016.
- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 4.5.2016, p. 1-88.
- European Commission, Commission communication, 'Strengthening Europe's cyber resilience system and fostering a competitive and innovative cybersecurity industry' (COM(2016) 410 final), Brussels, 5 July 2016.
- European Commission, Commission decision on the signing of a contractual arrangement on a public-private partnership for cybersecurity industrial research and innovation between the European Union, represented by the Commission, and the stakeholder organisation (C(2016) 4400 final), Brussels, 5 July 2016.
- European Commission and High Representative of the Union for Foreign Affairs and Security Policy, joint staff working document, 'EU operational protocol for countering hybrid threats: "EU Playbook"' (SWD(2016) 227 final), Brussels, 5 July 2016.
- Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (the NIS directive), OJ L 194, 19.7.2016, p. 1-30.
- European Commission, Commission communication, 'Space strategy for Europe' (COM(2016) 705 final), Brussels, 26 October 2016.
- European Commission, Commission communication, 'European defence action plan' (COM(2016) 950 final), Brussels, 30 November 2016.
- European Commission, Commission communication, 'Mid-term review on the implementation of the digital single market strategy: a connected digital single market for all' (COM(2017) 228 final), Brussels, 10 May 2017.
- Council of the European Union, Council conclusions on a framework for a joint EU diplomatic response to malicious cyber activities ('Cyber Diplomacy Toolbox') (9916/17), Brussels, 7 June 2017.
- European Commission, 'Reflection paper on the future of European defence' (COM(2017) 315 final), Brussels, 7 June 2017.
- EEAS, *Integrating cyber security in the planning and conduct of civilian CSDP missions* (Document ST 10548 2017 INIT), 21 June 2017.
- European Commission and High Representative of the Union for Foreign Affairs and Security Policy, joint report, *The implementation of the Joint Framework on countering hybrid threats — A European Union response* (JOIN(2017) 30 final), Brussels, 19 July 2017.
- European Commission, Commission Recommendation (EU) 2017/1584 on coordinated response to large-scale cybersecurity incidents and crises, Brussels, 13 September 2017.
- European Commission, Commission Recommendation (EU) 2019/553 on cybersecurity in the energy sector (notified under document C(2019) 2400), Brussels, 3 April 2019.

2.6 Chemical, biological, radiological, nuclear and high-yield explosive threats

2.6.1 What are chemical, biological, radiological, nuclear and high-yield explosive hazardous materials?

CBRN-E hazardous materials pose a major threat against which the EU must be prepared. Some chemicals, in particular toxic industrial materials, can cause burns and blisters, prevent breathing or attack the central nervous system. The biological agents in question are highly pathogenic bacteria and viruses or toxins affecting human health in a variety of ways. Ionising radiation arises from nuclear materials or other sources

of radiation, particularly from hospitals or industries, and can damage tissues and organs. The use of explosives in busy places is unfortunately well known. These materials are very dangerous and may hurt many people. CBRN-E events can happen accidentally, for example the sudden outbreak of an epidemic or the occurrence of an industrial catastrophe involving CBRN-E materials (e.g. the notorious incidents at Chernobyl or Fukushima, the explosion of the AZF factory in Toulouse, the leak of toxic sludge in Hungary), but there are increasing concerns about criminal use of CBRN-E materials.

When used on purpose, CBRN-E materials can become weapons of mass destruction. CBRN-E materials may lead to mass casualties, have long-term effects and create an extremely hazardous environment. The use of CBRN-E weapons is not new but has evolved over time. In the 18th century, the distribution of smallpox infected blankets deliberately contaminated the Native American population (Ranlet, 2000; see also Carus (2017) for an overview of biological warfare throughout history). Nuclear weapons have been used twice, as we all remember. Chemical weapons made their terrible appearance during the First World War and their use has recurred regularly since; we have all seen the horrific photographs from the Vietnam War or of the Halabja massacre in Iraq. Chemical weapons are still being used repeatedly today in Syria, in spite of an international ban. Chemical or radiological agents can also be used by clandestine criminals to kill targeted persons, as illustrated recently by the Novichok attack on Sergei and Julia Skripal in the United Kingdom and the assassination of the half-brother of the North Korean leader with a highly toxic chemical weapon in Kuala Lumpur in 2017.

CBRN-E incidents are frightening threats faced by our society. Owing to modern technology, the production of hazardous substances is easier now than it was a few years ago and thus the probability of an incident has of course increased. CBRN-E incidents may result from a disaster, but they may also be caused by non-state actors, that is, terrorists. Industrial and agricultural toxic chemicals can be purchased relatively cheaply and easily in most parts of the world. Illicit transfers have considerably increased, in parallel with the intensification of international commercial exchanges.

2.6.2 The European Union scene

To secure CBRN-E materials within the EU, the European Commission presented in 2009 a communication⁽¹⁰²⁾ on strengthening CBRN security in the Union, including an EU CBRN action plan (2009-2015) with 124 actions to complement national measures on prevention, detection, preparedness and response to CBRN incidents. Communications on new EU approaches to the detection and mitigation of CBRN-E risks followed in 2014 and 2017⁽¹⁰³⁾ with the aims of ensuring that unauthorised access to CBRN-E materials becomes ever more difficult and of developing better capacities to detect those materials and respond quickly and efficiently to CBRN-E events.

Threats to population health can emerge from multiple sources, including emerging or current pathogens but also chemical or radiological and nuclear events. In 2013, the EU adopted new legislation on cross-border threats to health⁽¹⁰⁴⁾, to improve preparedness across the EU and strengthen capacity to coordinate responses to health emergencies.

To limit the general public's ability to manufacture illicit explosives, a regulation was adopted harmonising rules concerning the availability, introduction, possession and use of substances or mixtures that could be misused and ensuring appropriate reporting on suspicious transactions throughout the supply chain⁽¹⁰⁵⁾.

To prevent the dissemination of CBRN-E materials outside the EU, the European Commission controls the export, transit and brokering of dual-use items (goods, software and technology that can be used for both civilian and military applications) with the aim of contributing to international peace and security and preventing the proliferation of weapons of mass destruction. The EU export controls⁽¹⁰⁶⁾ reflect commitments

⁽¹⁰²⁾ European Commission, Commission communication, 'Strengthening chemical, biological, radiological and nuclear security in the European Union — an EU CBRN action plan' (COM(2009) 273 final), Brussels, 24.6.2009.

⁽¹⁰³⁾ European Commission, Commission communication, 'New EU approach to the detection and mitigation of CBRN-E risks' (COM(2014) 247 final), Brussels, 5.5.2014; European Commission, Commission communication, 'Action plan to enhance preparedness against chemical, biological, radiological and nuclear security risks' (COM(2017) 610 final), Brussels, 18.10.2017.

⁽¹⁰⁴⁾ Decision No 1082/2013/EU of the European Parliament and of the Council of 22 October 2013 on serious cross-border threats to health and repealing Decision No 2119/98/EC, OJ L 293, 5.11.2013, p. 1-15.

⁽¹⁰⁵⁾ Regulation (EU) No 98/2013 of the European Parliament and of the Council of 15 January 2013 on the marketing and use of explosives precursors, OJ L 39, 9.2.2013, p. 1-11.

⁽¹⁰⁶⁾ Council Regulation (EC) No 428/2009 of 5 May 2009 setting up a Community regime for the control of exports, transfer, brokering and transit of dual-use items, OJ L 134, 29.5.2009, p. 1-269 (recast in 2017).

agreed upon in key multilateral export control regimes such as the Australia Group, the Wassenaar Arrangement, the Nuclear Suppliers Group and the Missile Technology Control Regime.

Dual-use items may be traded freely within the EU, except for some particularly sensitive items the transfer of which within the EU remains subject to prior authorisation. The directive of 2009⁽¹⁰⁷⁾ specifies the terms and conditions for transfers of defence-related products and provides a list of defence-related products that are subject to authorisation and licensing procedures. Items listed on the Common Military List of the European Union⁽¹⁰⁸⁾ include chemical or biological toxic agents, riot control agents, radioactive materials, and related equipment, components and materials.

Finally, the CBRN CoE initiative⁽¹⁰⁹⁾, funded by the IcSP (2014-2020)⁽¹¹⁰⁾, focusing particularly on crisis preparedness and response outside the EU, aims to mitigate risks related to CBRN-E materials. The causes of CBRN-E incidents can be natural, accidental or intentional, but it is in particular the intentional or malevolent use of those materials for terrorist attacks that is of increasing concern to the EU.

The EU needs to position itself to stay ahead of an ever-evolving CBRN-E threat. An obvious first line of defence is to prevent as far as possible access to CBRN-E materials, securing correctly chemical and nuclear plants, pharmaceutical laboratories, agro-chemical storage spaces and other dangerous facilities in the EU but also outside it, in neighbouring countries, and preventing the potential introduction of dangerous ingredients and equipment into the EU. Limited access should be accompanied by appropriate vetting of on-site workers. Similarly, stricter control of trade in dual-use products should be properly enforced. Preparedness is also an important component of the answer, and a precise chain of command needs to be in place in case of a CBRN-E incident; there also needs to be sufficient availability of skilled people with the necessary equipment. A common vision between countries is essential, since CBRN-E incidents extend across borders.

2.6.3 International agreements

The Chemical Weapons Convention⁽¹¹¹⁾, which entered into force in 1997, aims to eliminate chemical weapons of mass destruction by prohibiting the development, production, acquisition, stockpiling, retention, transfer or use of chemical weapons by states parties. States parties must take the necessary steps to enforce that prohibition within their jurisdiction. The convention also regulates the destruction of chemical weapons and shut-down of production facilities. The development and production of several substances (and precursors) are subject to limits and inspections. In case of doubt about states' compliance (Article IX) and where assistance and protection are needed (Article X), including emergency protection against chemical weapons and riot control agents, an investigation procedure is conducted following the Verification Annex, Part XI. Implementation is monitored by the Organisation for the Prohibition of Chemical Weapons.

The Biological and Toxin Weapons Convention (BTWC or BWC)⁽¹¹²⁾ entered into force in March 1975; it prohibits the development, production, stockpiling, acquisition or retention of microbial and biological agents and toxins — unless for peaceful purposes — and of weapons, equipment and means of delivery of such agents for hostile purposes. According to the BTWC, the parties shall prohibit any actor from such activities; however, the exchange of equipment and information for the peaceful use of such agents must be supported. Surveillance and detection of infectious diseases in case of danger should be coordinated by intergovernmental organisations (e.g. the World Health Organization (WHO)). The BTWC has a peer complaint reporting system to enable complaints to the UN Security Council in case of a suspected breach, and there is also an investigation mechanism. The Implementation Support Unit, housed within the UN Office for Disarmament, receives information on national legislation, matches requests for assistance from the states and links national contact points.

⁽¹⁰⁷⁾ Directive 2009/43/EC of the European Parliament and of the Council of 6 May 2009 simplifying terms and conditions of transfers of defence-related products within the Community, OJ L 146, 10.6.2009, p. 1-36.

⁽¹⁰⁸⁾ Council of the European Union, Common Military List of the European Union adopted by the Council on 9 February 2015 (equipment covered by Council common position 2008/944/CFSP defining common rules governing the control of exports of military technology and equipment), OJ C 129, 21 April 2015.

⁽¹⁰⁹⁾ European Commission, 'EU Chemical, Biological, Radiological, and Nuclear Risk Mitigation Centres of Excellence (CoE)' (<http://www.cbrn-coe.eu/>).

⁽¹¹⁰⁾ European Commission, 'Service for Foreign Policy Instruments (FPI)' (http://ec.europa.eu/dgs/fpi/documents/140311_icsp_reg_230_2014_en.pdf).

⁽¹¹¹⁾ Organisation for the Prohibition of Chemical Weapons, 'Chemical Weapons Convention' (<https://www.opcw.org/chemical-weapons-convention>).

⁽¹¹²⁾ UN Office for Disarmament Affairs, 'Biological weapons: the Biological Weapons Convention' (<https://www.un.org/disarmament/wmd/bio/>).

In response to the exponential increase in international travel and trade, and the emergence and re-emergence of international diseases and other health risks, 194 countries across the globe have agreed to implement the International Health Regulations (WHO, 2007). Members of WHO must report disease outbreaks. The aim of the regulations is to provide a public health response to emergencies.

The Treaty on the Non-Proliferation of Nuclear Weapons (¹¹³) was opened for signature in 1968 and entered into force in 1970, and since that time 191 parties, including the five nuclear-weapon states, have joined. The objectives are to prevent the spread of nuclear weapons and weapons technology and to further the goal of achieving nuclear disarmament and general and complete disarmament.

The International Atomic Energy Agency (IAEA) Convention on the Physical Protection of Nuclear Material and Nuclear Facilities (¹¹⁴) regulates the physical protection regime for nuclear material (use, storage and transport) and nuclear facilities both used for peaceful purposes. The countries that have signed the convention must set up an adequate protection regime for material and facilities, including the capacity to locate and recover missing or stolen material and to protect against sabotage.

According to the International Civil Aviation Organisation Convention on the Marking of Plastic Explosives for the Purpose of Detection (¹¹⁵), signed in 1991 and which entered into force in June 1998, each state party must prohibit and prevent the manufacture in its territory of unmarked plastic explosives. Plastic explosives are to be marked by introducing during the manufacturing process any one of four agreed detection agents (listed in the technical annex). Each state party must prohibit and prevent the movement into or out of its territory of unmarked explosives and exercise strict and effective control over the possession of any existing stocks of unmarked explosives. Stocks of plastic explosives not held by authorities performing military and police functions are to be destroyed, marked or rendered permanently ineffective.

UN Security Council Resolution 1540 of 2004 (UN Security Council, 2004) addresses the non-proliferation of weapons of mass destruction and requires all UN Member States to impede the development, acquisition, manufacture, possession, transport, transfer or use of nuclear, chemical or biological weapons and means of delivery by non-state actors. States must take active measures to establish domestic controls, develop effective border controls and combat illicit trafficking. States have to establish effective national export and trans-shipment controls over such items. A 1540 Committee has been established to supervise the implementation of the resolution.

2.6.4 Possible evolution within the next 5 years

There is a potential risk that terrorist groups or non-state actors will use CBRN-E materials in future attacks in Europe, with a higher probability for chemical or biological weapons. The security of such material is therefore a crucial issue, and thefts and losses occur on hundreds of occasions each year.

Dual-use products such as pesticides can also be accessed through chemical stockpiles in unstable countries. Toxic chemicals are the perfect weapon for our fake-news world, where responsibility is often in doubt and provenance hard to pinpoint. In addition, the advent of molecular biology techniques has allowed easier manipulation of bacteria and viruses, providing the means to create antibiotic- or antiviral-resistant pathogens or to synthesise pathogenic organisms without having to source the organisms themselves.

Last but not least, drones could be used for the dispersal of such material. Small drones are cheap, easy to buy and operate, and can provide distance and anonymity to their operators. Drones have proliferated on a massive scale and improvements in battery technology give them greater power, lift and endurance, while fast chips and sensors allow automatic stability and easy operation.

Terrorist incidents cause a higher level of psychopathology than those occasioned by natural disasters, but it would be even worse if CBRN-E materials were involved in an attack.

(¹¹³) UN Office for Disarmament Affairs, 'Treaty on the Non-Proliferation of Nuclear Weapons' (<https://www.un.org/disarmament/wmd/nuclear/npt/>).

(¹¹⁴) IAEA, 'Convention on the Physical Protection of Nuclear Material' (<https://www.iaea.org/publications/documents/conventions/convention-physical-protection-nuclear-material>).

(¹¹⁵) International Civil Aviation Organisation, 'Convention on the Marking of Plastic Explosives for the Purposes of Detection' (https://www.icao.int/secretariat/legal/List%20of%20Parties/MEX_EN.pdf).

2.6.5 Stakeholders

2.6.5.1 European Union stakeholders

European Commission Directorate-General for Migration and Home Affairs

The EU agenda on security⁽¹¹⁶⁾ aims to strengthen the tools that the EU provides to national law enforcement authorities to fight terrorism and cross-border crime. In particular, DG Migration and Home Affairs is responsible for the EU CBRN action plan and related activities. In order to assist the Commission in its tasks, a CBRN Advisory Group, created in 2010, brings together the CBRN security coordinators of all the Member States.

https://ec.europa.eu/home-affairs/what-we-do/policies/crisis-and-terrorism/securing-dangerous-material_en

European Commission Directorate-General for Trade

DG Trade is in charge of Regulation (EC) No 428/2009, which governs the EU's export control regime. It contains a common EU list of dual-use items and a 'catch-all clause' for non-listed items in connection with a weapons of mass destruction programme (including CBRN items). This regulation calls for an annual report on the activities of the Dual-Use Coordination Group. Through the CBRN CoE initiative, a programme has been set up to enhance outreach to partner countries on export control of dual-use items (the EU-P2P export control programme; the website is run by the JRC)⁽¹¹⁷⁾.

<http://ec.europa.eu/trade/import-and-export-rules/export-from-eu/dual-use-controls/>

European Commission Directorate-General for Health and Food Safety

Public health emergencies at EU level are managed under the legislation on cross-border threats to health from 2013⁽¹¹⁸⁾, which provides for a comprehensive and coordinated approach to preparedness, early warning, risk assessment and crisis response. The Early Warning and Response System is a tool managed by the European Centre for Disease Prevention and Control (with restricted access) to monitor public health threats in the EU in order to ensure a rapid and effective response to health events (including emergencies). The Health Security Committee is a body responsible for the coordination of health security measures in the EU, including CBRN-related measures⁽¹¹⁹⁾.

https://ec.europa.eu/health/preparedness_response/risk_management/hsc_en

European Commission Directorate-General for International Cooperation and Development

DG International Cooperation and Development supports the implementation of the EU CBRN CoE initiative, a worldwide programme involving 61 partner countries financed under the EU's IcSP. The DG also implements the EU-P2P export control programme described above.

https://ec.europa.eu/europeaid/tags/centres-excellence-cbrn_en

European Commission Directorate-General for European Civil Protection and Humanitarian Aid Operations (ECHO)

Under the EU's Civil Protection Mechanism⁽¹²⁰⁾, the EU offers assistance to respond to major emergencies and to enhance preventive and preparedness measures for all kinds of emergencies, including CBRN disasters. Within the framework of the mechanism, there are 17 training modules dedicated to civil protection workers; one focuses on CBRN detection and sampling, and another is dedicated to search and rescue in CBRN conditions. ECHO also organises regular trans-border exercises, including on CBRN incidents.

https://ec.europa.eu/echo/what/civil-protection/mechanism_en

⁽¹¹⁶⁾ European Commission communication COM(2015) 185 final.

⁽¹¹⁷⁾ European Commission, 'EU P2P (partner to partner) export controls programme' (<https://export-control.jrc.ec.europa.eu/>).

⁽¹¹⁸⁾ Decision No 1082/2013/EU.

⁽¹¹⁹⁾ European Commission, Commission staff working document, 'Health security in the European Union and internationally' (SEC(2009) 1622 final), Brussels, 23.11.2009.

⁽¹²⁰⁾ Decision No 1313/2013/EU of the European Parliament and of the Council of 17 December 2013 on a Union civil protection mechanism, Brussels, OJ L 347, 20.12.2013, p. 924-947.

European Commission Directorate-General Joint Research Centre

The JRC is the European Commission's science and knowledge service. It has solid research and policy support experience, developed in house, as well as broad networks with academia, industry, Member States and city authorities. The JRC has been active for many years in the vast area of CBRN-E threats. Details are presented in Section 3.4.

<https://ec.europa.eu/jrc/en/research-topic/chemical-biological-radiological-and-nuclear-hazards>

European Defence Agency

The EDA was created in 2004; all the Member States except Denmark participate. The agency aims to improve the EU's defence capabilities through cooperative projects and programmes. The European Framework Cooperation for Security and Defence involves cooperation between the EDA and the European Commission on CBRN research, with a joint investment programme having been established in 2010. The investment programme launched 2 calls for projects in 2012 and 2013, with 14 projects selected and a budget of EUR 12 million (12 projects were still running in 2016, according to the EDA website, consulted on 16 January 2019). Research topics include the remote detection of chemical threats, point detection of biological threats, handling mixed CBRN samples, modelling and simulation of CBRN architectures, decontamination management and sensor networking for CBRN.

<https://www.eda.europa.eu/>

European Union Agency for Law Enforcement Cooperation (Europol)

Europol supports law enforcement authorities in their crime-fighting activities to achieve a safer Europe for all citizens. The main current threats include cybercrime and trafficking in human beings. Europol manages the EU Bomb Data System for sharing technical information and intelligence on explosives and CBRN (with two different multilingual databases). The European Explosive Ordnance Disposal Network (EEODN) is a Europol platform for experts established in 2008 to fight against terrorism. Through this platform, Europol enhances and develops knowledge in the field of (CBRN-E) security, by facilitating the sharing of best practices among EU experts (Europol, 2018a). Explosive ordnance disposal and CBRN experts meet twice a year to discuss and explore existing threats from the illicit use of explosives and CBRN agents. The EEODN is also intended to improve civil-military cooperation between competent authorities in the field of explosives and CBRN.

Since 2013, these activities have been incorporated in the training portfolio of the European Union Agency for Law Enforcement Training (CEPOL).

<https://www.europol.europa.eu/> and <https://www.cepol.europa.eu/>

European Centre for Disease Prevention and Control

This EU agency, established in 2005, aims to strengthen Europe's defences against infectious diseases and develops, with Member States, disease surveillance and early warning systems. At CBRN level, it ensures cross-sectoral bio-risk awareness and mitigation training, produces a handbook on the threat posed by bioterrorism, and raises awareness and disseminates best practices as regards 'do it yourself' biology.

<https://ecdc.europa.eu/en/home>

European Food Safety Authority

This EU agency ensures the safety of the EU food chain by providing scientific advice to risk managers, by communicating with the public about risks and by cooperating with Member States and other parties to deliver a coherent, trusted food safety system in the EU. In the event of an incident of malevolent food poisoning, the European Food Safety Authority would have to assess the related risks.

<http://www.efsa.europa.eu/>

European Biosafety Association (EBSA)

The not-for-profit organisation EBSA, founded in 1996, establishes and communicates best biosafety and biosecurity practices among its members and encourages dialogue and discussions on developing issues. EBSA has several focal points, one of which deals with BTWC/CBRN matters.

<http://ebsaweb.eu/focal-points>

2.6.5.2 International stakeholders

International Atomic Energy Agency

The IAEA is an independent intergovernmental, science- and technology-based organisation, within the UN, and serves as the global focal point for nuclear cooperation. The IAEA:

- assists Member States in using nuclear science and technology for peaceful purposes (including the generation of electricity), and facilitates the transfer of technology and knowledge in a sustainable manner to developing member states;
- develops nuclear safety standards and promotes the achievement and maintenance of high levels of safety in applications of nuclear energy, as well as the protection of human health and the environment against ionising radiation;
- verifies, through its inspection system, that states comply with their commitments under the Treaty on Non-Proliferation of Nuclear Weapons and other non-proliferation agreements to use nuclear material and facilities only for peaceful purposes.

Border Monitoring Working Group

This working group was established in 2005 by IAEA, the European Union and the United States to promote co-operation between its members and serve as a forum for discussion and exchange of information on plans and programs to be implemented by the members in cooperation with the recipient countries to combat the illicit trafficking of nuclear and other radioactive material that is out of regulatory control.

<https://www.iaea.org/>

International Criminal Police Organisation (Interpol)

This international organisation, established in 1956, enables police around the world to work together (currently it has 194 member states). It provides expertise and capabilities through three main programmes: counterterrorism, cybercrime, and organised and emerging crime. One of the 'crime areas' identified by the organisation is CBRN-E and the prevention of CBRN-E terrorism thanks to (i) sharing information and intelligence analysis, (ii) capacity building and training, and (iii) operational and investigative support. Activities include data analysis, training workshops, table-top exercises, international conferences and on-the-ground operations.

<https://www.interpol.int/>

United Nations Interregional Crime and Justice Research Institute

The UN Interregional Crime and Justice Research Institute (1968) aims to implement improved policies and actions in the field of crime prevention and control:

- to advance understanding of crime-related problems;
- to foster just and efficient criminal justice systems;
- to support respect for international instruments and other standards;
- to facilitate international law enforcement cooperation and judicial assistance.

The institute, through its CBRN risk mitigation and security governance programme, supports the development of an integrated CBRN approach through which all stakeholders, while operating autonomously, can establish common goals, identify and manage resources to achieve them, and clearly allocate responsibilities and tasks.

<http://www.unicri.it>

The Global Partnership against the Spread of Weapons and Materials of Mass Destruction

The Global Partnership, established in 2002, is an international initiative (currently with 31 active members) that contributes to international security through specific cooperation projects to:

- secure and destroy dangerous CBRN materials;
- protect vulnerable physical infrastructure;

- strengthen global networks, supporting international initiatives such as the Nuclear Security Summit and the Global Health Security Agenda (GHSA);
- build partner capacity to meet the international obligations set out in UN Security Council Resolution 1540 against the proliferation of weapons of mass destruction (UN Security Council, 2004).

The Global Partnership is committed to preventing CBRN terrorism and proliferation.

<https://www.gpwmd.com/cbrnwg>

Organization for Security and Co-operation in Europe

The OSCE takes an inclusive approach to security that includes politico-military, economic, environmental and human aspects. It addresses a wide range of security-related concerns, arms control, human rights, confidence- and security-building measures, national minorities, democratisation, policing strategies, counterterrorism, and economic and environmental activities. The 57 participating states enjoy equal status; decisions are taken by consensus on a politically but not legally binding basis. Most OSCE field operations are deployed in south-eastern Europe, the south Caucasus and central Asia. Within the CBRN field, the OSCE is active in counterterrorism and border control.

<https://www.osce.org/>

North Atlantic Treaty Organization

NATO is an intergovernmental military alliance between 29 North American and European countries, under a treaty signed in 1949. NATO is a system of collective defence whereby its member states agree to mutual defence in response to an attack by any external party. The proliferation of weapons of mass destruction and their delivery systems are among the current threats.

The NATO Joint CBRN Defence Task Force consists of a CBRN Joint Assessment Team and a CBRN Defence Battalion. This battalion is trained and equipped to deal with CBRN events not only in armed conflicts but also in crisis situations such as natural disasters and industrial accidents. *Guidelines and Minimum Standards for CBRN First Responders* have been produced by NATO's Civil Protection Group, supporting the planning and implementation of responses to CBRN incidents.

https://www.nato.int/cps/en/natolive/topics_49156.htm

World Health Organization

WHO, a United Nations agency, is a coordinating authority on international health with the following objectives (among others):

- monitoring the health situation;
- setting norms and standards and promoting their implementation;
- providing technical support and building sustainable institutional capacity;
- working with countries to respond to crisis and health emergencies.

WHO wishes to establish an integrated global alert and response system for epidemics and other public health emergencies. It supports its Member States in the implementation of national capacities for epidemic preparedness and response in the context of the International Health Regulations of 2005 (WHO, 2007), including laboratory capacities and early warning alert and response systems.

After the Ebola crisis in west Africa in 2014, WHO, together with the GHSA, developed the Joint External Evaluation tool as part of the International Health Regulations monitoring and evaluation framework. This tool is used to assess a country's capacity to prevent, detect and respond to public health threats, be they naturally occurring, deliberately caused or accidental. It has a section dedicated to biosafety and biosecurity, and another on chemical and radiological emergencies. A WHO manual on laboratory biosafety also provides guidelines. In addition, guidance documents on public health response to biological and chemical weapons and on laboratory biosecurity have been published. All the documents mentioned are available at the web address below.

<https://www.who.int/home>

Global Health Security Agenda

The GHSA, launched in 2014, is a partnership of nations, international organisations and non-governmental stakeholders to help build countries' capacity to create a world safe and secure from infectious disease threats and elevate global health security as a national and global priority. GHSA pursues a multilateral and multisectoral approach (criminal threats are included). It contributed to the development of the Joint External Evaluation tool described above.

<https://www.ghsagenda.org/about>

Global Health Security Initiative

The Global Health Security Initiative, launched in 2001, is an informal, international partnership to strengthen health preparedness and response globally to threats of biological, chemical or radionuclear terrorism and pandemic influenza. WHO serves as an expert adviser to the initiative.

<http://www.ghsi.ca/english/index.asp>

World Organisation for Animal Health (OIE)

The World Organisation for Animal Health, established in 1924 as the Office International des Épizooties, is responsible for improving animal health worldwide, with 182 member countries, and is a reference organisation for the World Trade Organization. Each member country reports animal diseases detected on its territory. The OIE disseminates the information to other countries, which can take the necessary preventive actions. This information provision also covers diseases transmissible to humans and intentional introduction of pathogens; the OIE takes very seriously the threat posed by accidental or deliberate release of animal pathogens (breaches of biosecurity). It should be noted that several OIE biosecurity programmes combating zoonoses such as avian influenza and Rift Valley fever and the spread of antibiotic resistance in developing countries are funded by the Food and Agriculture Organisation of the UN ⁽¹²¹⁾.

<http://www.oie.int/>

International Federation of Biosafety Associations (IFBA)

The IFBA, a not-for-profit non-governmental organisation (NGO) of biosafety associations from all over the world, has the mission of ensuring 'safe and secure work with biological materials'. Among its priorities, the development of innovative approaches to achieving affordable biosafety and biosecurity capacities appropriate to regions with limited resources is crucial. The IFBA is a GHSA partner, supporting the development of national biosafety and biosecurity strategies and guidelines, and certifying the competency of biosafety professionals handling infectious disease agents.

<https://www.internationalbiosafety.org/>

International regimes for the control of export of strategic goods

Various groups are listed hereafter.

- The Australia Group combats the proliferation of biological and chemical weapons (<https://australiagroup.net/en/>).
- The Missile Technology Control Regime regulates matters such as the export of missile components and components for unmanned aerial vehicles (<http://mtcr.info/>).
- The Nuclear Suppliers Group concludes agreements to prevent proliferation of nuclear goods and technologies (<http://www.nuclearsuppliersgroup.org/en/>).
- The Wassenaar Arrangement includes agreements on export controls for military and dual-use goods (<https://www.wassenaar.org/>).
- The Zangger Committee ensures that countries interpret the nuclear export control policies under the Treaty on Non-Proliferation of Nuclear Weapons in the same manner (<http://zanggercommittee.org/>).

⁽¹²¹⁾ Food and Agriculture Organisation of the United Nations 'Transboundary animal diseases' (<http://www.fao.org/emergencies/emergency-types/transboundary-animal-diseases/en/>).

Global Initiative to Combat Nuclear Terrorism (GICNT)

This Global Initiative is a voluntary international partnership of 89 nations and six international organizations that are committed to strengthening global capacity to prevent, detect, and respond to nuclear terrorism.

<http://www.gicnt.org/>

2.6.6 Legislation and reference documents

EU legislation

- The Euratom Treaty coordinates research on atomic energy, establishes a common market for nuclear equipment and materials, and sets out safety and health regulations. It operates an effective regional nuclear safeguards system, encompassing nuclear material accountancy, verification through on-site inspections, regular reporting, and technical and scientific support to EU Member States, in close partnership with the IAEA. It participates in the fight against the illicit trafficking of nuclear and radiological materials.
- Council of the European Union Regulation (EC) No 428/2009 of 5 May 2009 setting up a Community regime for the control of exports, transfer, brokering and transit of dual-use items, OJ L 134, 29.5.2009, p. 1-269 (recast in 2017).
- Directive 2009/43/EC of the European Parliament and of the Council of 6 May 2009 simplifying terms and conditions of transfers of defence-related products within the Community, OJ L 146, 10.6.2009, p. 1-36.
- European Commission, Commission communication, 'Strengthening chemical, biological, radiological and nuclear security in the European Union — an EU CBRN action plan' (COM(2009) 273 final), Brussels, 24 June 2009.
- Decision No 1082/2013/EU of the European Parliament and of the Council of 22 October 2013 on serious cross-border threats to health and repealing Decision No 2119/98/EC, OJ L 293, 5.11.2013, p. 1-15.
- European Commission, Commission communication, 'New EU approach to the detection and mitigation of CBRN-E risks' (COM(2014) 247 final), Brussels, 5 May 2014.
- Council of the European Union, Common Military List of the European Union adopted by the Council on 9 February 2015 (equipment covered by Council common position 2008/944/CFSP defining common rules governing the control of exports of military technology and equipment), OJ C 129, 21 April 2015.
- European Commission, Commission communication, 'Action plan to enhance preparedness against chemical, biological, radiological and nuclear security risks' (COM(2017) 610 final), Brussels, 18 October 2017.

International treaties related to CBRN-E issues

- Treaty on the Non-Proliferation of Nuclear Weapons, London, Moscow and Washington DC, 1 July 1968.
- Convention on the Prohibition of Development, Production and Stockpiling of Biological and Toxic Weapons and on their Destruction, London, Moscow and Washington DC, 10 April 1972.
- Convention on the Physical Protection of Nuclear Material, Vienna and New York, 3 March 1980.
- Convention on the Marking of Plastic Explosives for the Purpose of Detection, Montreal, 1 March 1991.
- Convention on the Prohibition of the Development, Production, Stockpiling and Use of Chemical Weapons and on their Destruction, Paris, 13 January 1993.
- Resolution 1540 of the UN Security Council, 28 April 2004.
- International Health Regulations (2005), Geneva, 2007.

For further details on legislation and stakeholders related to CBRN-E issues, Eurojust publishes a report dedicated to the topic, which is periodically updated (Eurojust, 2017).

2.7 Hybrid threats

2.7.1 What are hybrid threats?

The EU, the Member States and non-EU countries are increasingly exposed to hostile actions that are generically called ‘hybrid threats’. These aim not only to produce direct damage to and exploit the vulnerabilities of their adversaries or opponents but also to destabilise societies, regions or states and create ambiguity to hinder decision making. Territorial integrity and political sovereignty may also be at stake.

Although the concept of a hybrid threat is not quite new ⁽¹²²⁾, there is no single definition of what hybrid threats are. There is, however, general agreement in stating that these threats involve combinations of conventional and unconventional tools and tactics to destabilise the adversary. As the word implies, ‘hybrid’ means ‘of a nature that is the product of multiple sources (or ways of acting towards a definite objective)’; therefore, hybrid threats involve a mix of different approaches — conventional and unconventional, military and non-military, overt and covert — and actors — state entities and non-state groups — gathered to threaten or attack chosen targets. Depending on the levels of intensity of the threat and the motivation of the actors involved, it is possible to further distinguish between a hybrid threat, a hybrid conflict and hybrid warfare, with the last two being specific categories in which some hybrid tactics are used by a state to achieve its strategic ends (Hoffmann, 2014; European Parliament, 2015a).

At the EU level, a formal definition of hybrid threats is found in a joint communication of the European Commission and the High Representative of the Union for Foreign Affairs and Security Policy of 2016: ‘the concept [of hybrid threats] aims to capture the mixture of coercive and subversive activity, conventional and unconventional methods (i.e. diplomatic, military, economic, technological), which can be used in a coordinated manner by state or non-state actors to achieve specific objectives while remaining below the threshold of formally declared warfare.’ ⁽¹²³⁾. In a later joint communication of the European Parliament, the European Council and the Council, of 2018, reference is made to ‘hybrid campaigns’, a term that further highlights their multidimensional and complex nature ⁽¹²⁴⁾.

Not all present-day threats can be described as hybrid. The notion of composite origin is paramount here. To give an example, a terrorist group that mainly plants bombs does not qualify as a hybrid threat. However, the combination of such bombing with, for instance, disinformation campaigns or criminal activities would transform a mono-threat into a hybrid one. Similarly, cybercrime and human trafficking, for instance, are not hybrid by their very nature, but they may easily become hybrid threats through association with other attack modes (Andersson and Tardy, 2015). To put it another way, hybrid threats constitute a synthesis of attack scenarios long regarded as isolated.

It is also important be aware that a hybrid threat does not necessarily include force of arms. It can appear without the use of physical force, but it has to include a combination of non-violent practices to be considered a hybrid threat (Dengg and Schurian, 2006).

2.7.2 How do hybrid attackers operate?

The rhizomatic structure of hybrid threats is also reflected in the variety of *modus operandi* used by hybrid aggressors, which societies and their authorities must cope with in reacting to such threats (e.g. through preventive and preparedness actions). This then brings greater levels of complexity than in single threats. Thorough descriptions of such action modes have been published (see, for example, Giannopoulos et al., 2018) and will be summarised hereafter. Three main ‘blocks’ of a given entity such as a state or a region are often targeted during hybrid attacks — the infrastructures (critical infrastructures but also public spaces), the media and communication systems (through manipulation, disinformation campaigns, etc.) — thus taking advantage of potential societal vulnerabilities.

Infrastructures, in particular for energy, transport, space, defence and communications, are obvious and attractive targets for hybrid attacks aimed at degrading their availability and reliability, in order to induce social frustration, fear and vulnerability. As an illustration, we might mention the now exemplary cyberattacks

⁽¹²²⁾ Andersson and Tardy (2015) state correctly that ‘warfare itself has never been “pure”’. It is also true that modern technology capacities and dependencies facilitate and multiply the potency and devastating impacts of hybrid threats.

⁽¹²³⁾ European Commission and High Representative of the Union for Foreign Affairs and Security Policy, joint communication, ‘Joint framework on countering hybrid threats: a European Union response’ (JOIN(2016) 18 final), Brussels, 16.4.2016.

⁽¹²⁴⁾ European Parliament, European Council and Council joint communication, ‘Increasing resilience and bolstering capabilities to address hybrid threats’ (JOIN(2018) 16 final), Brussels, 13.6.2018.

against Ukraine's electricity infrastructure, which temporarily disrupted electricity supply to over 225 000 consumers in December 2015, demonstrating the capability of the adversary to strongly impact one of the country's core infrastructures (Styczinski et al., 2016). Another example of such attacks, again against Ukraine, is the part of the Russian invasion of Crimea that involved local military action (conducted by special operations forces) supported by disinformation campaigns and cyberattacks: the occupation of the Simferopol internet exchange point, followed by the disruption of cable connections to the mainland, secured Russian information dominance in the peninsula, which was combined with informational and psychological warfare targeting Ukraine and the EU (Canadian Security Intelligence Service, 2018).

As can be seen from the previous examples, media manipulation, propaganda and disinformation campaigns through social media or other means are an indispensable part of hybrid threats. The new information age provides opportunities in this regard that were considered simply impossible some years ago. The rapid proliferation of smartphones and all their technical capabilities — such as saving and sending videos and photographs or information — enable the worldwide provision of information — real or fake — by any user with scarcely any delay. Disinformation, regardless of the entity engaging in the activity, is aggressive marketing of information in support of political objectives and, as part of a hybrid threat, serves to steer people's thinking in the direction desired by the attacker. Recent examples are numerous (see, for example, Canadian Security Intelligence Service, 2018; Trevorton et al., 2018).

Furthermore, hybrid threats will always try to take advantage of societal weaknesses and vulnerabilities that may exist structurally or temporarily within their intended targets. These vulnerabilities can be the outcome of very different situations or developments, such as historical memory, legislation, old practices, geostrategic factors, a high degree of polarisation of society, technological disadvantages or ideological differences. In some situations, adversaries will identify these vulnerabilities and exploit them to create ambiguity and confusion and instil fear among citizens and authorities in the targeted countries. This is, for instance, what Islamic State in Iraq and the Levant (ISIL, sometimes referred to as ISIS or Daesh) did with EU citizens and governments, pushing them to take more hostile attitudes towards refugees, ultimately strengthening the image of the EU as an anti-Muslim society, to its discredit, promoting, in the end, radicalisation of people who would later support the deployment of targeted terrorist attacks.

Recently, and in order to provide further clarity on this topic, the JRC and the Centre of Excellence for Countering Hybrid Threats (Hybrid CoE) have jointly developed a conceptual framework (Giannopoulos et al., 2019) that aims to characterise hybrid threats and foster a better understanding among the various stakeholders. This framework is based on five pillars providing answers to (1) who might be behind hybrid activity, (2) the means that can be used (tools), (3) the areas that can be targeted and affected (domains), (4) the evolution timeline and (5) the objectives of hybrid activities. A hybrid actor might be a state actor or a non-state actor (e.g. a terrorist organisation, a transnational criminal organisation or a private military organisation) or a proxy acting on behalf of another hybrid actor.

The hybrid threat is an overarching concept that incorporates different types of activity and an escalation process with a number of phases. The phases are priming, destabilisation and coercion. Activities in the phases can sometimes overlap. While there is always escalation potential, this does not mean that all hybrid campaigns will escalate to the coercion phase. On the contrary, an actor may perform persistent priming for long periods of time. The activities observed in the different phases are interference, influence, operations/campaign and warfare. Interference and influence usually belong to the priming phase; influence and operations/campaigns are features of the destabilisation phase; and the coercion phase may include hybrid operations/campaigns and warfare.

As mentioned above, hybrid attackers select a number of tools to affect one or more of a country's domains. Thirteen domains have been identified, coupled with a (non-exhaustive) list of tools that can be used to affect these domains. An adversary selects tools to achieve strategic objectives. These form a hybrid toolbox, which may vary depending on the adversary (state actor, non-state actor or proxy). Each tool targets one or multiple domains or the interface between them. Tools can exploit the vulnerability of a domain or domains or take advantage of an opportunity. The objective can be achieved either by the direct effect of the tool on the domain or through the resulting cascade effects. Such tools might be technological ones (e.g. cyberattacks) but they might also relate to the media, propaganda, etc.

2.7.3 Countering hybrid threats in the European Union

Finding the right responses to counter hybrid threats requires the establishment of an array of strategies and tools, because of the variety of channels that need to be followed simultaneously. Responses must also take into consideration the interconnected nature of the challenges (e.g. ethnic conflict, terrorism, migration and weak institutions), the multiplicity of actors (e.g. regular and irregular forces, criminal groups) and the diversity of conventional and unconventional means used (e.g. military, diplomatic, technological) (European Parliament, 2015a).

Countering hybrid threats also means countering ambiguity, confusion and fear deliberately created by adversaries in the targeted entity in order to hinder or block democratic decision making and enable them to perform their malicious acts. As correctly indicated by the title of a recent NATO report called *Hybrid Threats: Overcoming ambiguity, building resilience* (NATO Energy Security Centre of Excellence, 2017), ensuring resilience at every level of societies and states must be at the core of strategies to be adopted and implemented by democratic nations and alliances of nations.

This is the path followed by the European Commission and the HR/VP, who adopted in 2016 a joint framework to counter hybrid threats and foster the resilience of the EU, its Member States and partner countries while increasing cooperation with NATO on countering these threats. This framework, through the actions it proposes, envisages work along four lines ⁽¹²⁵⁾:

1. raising awareness by establishing dedicated mechanisms for the exchange of information between Member States and by coordinating EU actions to deliver strategic communication;
2. building resilience by addressing potential strategic and critical sectors such as cybersecurity, critical infrastructures, protection of the financial system and protection of public health, and supporting efforts to counter violent extremism and radicalisation;
3. preventing threats, responding to crisis and recovering by defining effective procedures to follow, but also by examining the applicability and practical implications of the Solidarity Clause (Article 222 of the TFEU) and the mutual defence clause (Article 42(7) of the Treaty on European Union), in the event that a wide-ranging and serious hybrid attack occurs;
4. stepping up cooperation between the EU and NATO as well as other partner organisations, in a joint effort to counter hybrid threats, while respecting the principles of inclusiveness and the autonomy of each organisation's decision-making process.

As far as the EU is concerned, countering hybrid threats is largely a matter of Member State competence; Member States must develop integrated national responses, including threat analysis, self-assessment of vulnerabilities and a comprehensive security approach. However, the joint framework adopted 2 years ago aims to help EU Member States and their partners to counter hybrid threats and increase their resilience when facing them by combining European and national instruments in a more effective way than in the past. The first report on the implementation of the joint framework was issued in July 2017 ⁽¹²⁶⁾ and updated 1 year later ⁽¹²⁷⁾; it puts a strong emphasis in particular on the CBRN-E aspects of hybrid threats.

On the whole, an integrated international response, including joint EU and NATO efforts, is much needed to support the assessment of threats and vulnerabilities as well as coordinated action. Efforts in this regard are described further in Section 2.7.5.

2.7.4 Possible evolution of hybrid threats within the next 5 years

Hybrid threats are not expected to diminish; on the contrary, they are expected to increase in number and complexity. This trend can be attributed to the fact that adversaries are becoming more technologically advanced and experienced in conducting such threats. In addition, the enablers of hybrid threats (mainly technological means such as cyberattacks, but also disinformation and propaganda) are accessible by state

⁽¹²⁵⁾ For details, see European Commission and High Representative joint communication JOIN(2016) 18 final.

⁽¹²⁶⁾ European Commission and High Representative of the Union for Foreign Affairs and Security Policy, joint report, *The implementation of the joint framework on countering hybrid threats — A European Union response* (JOIN(2017) 30 final), Brussels, 19.7.2017.

⁽¹²⁷⁾ European Commission and High Representative of the Union for Foreign Affairs and Security Policy, joint report, *The implementation of the joint framework on countering hybrid threats from July 2017 to June 2018* (JOIN(2018) 14 final), Brussels, 13.6.2018.

and non-state actors. To a certain extent, hybrid threats enable relatively small terrorist groups and/or poor countries to be more effective than their resources would ever have allowed them to be in the past.

The evolution of hybrid threats will be closely linked to how societal weakness manifests itself in European countries. Hybrid threats are more effective in countries that face severe societal challenges. The capability of EU Member States to address such issues will define to a large extent their vulnerability against hybrid threats. Issues related to emerging technologies and trends, such as digitalisation, will certainly determine new channels of attack and affect how Member States perceive and respond to hybrid threats.

It is also expected that the ways in which countries respond to hybrid threats will change dramatically. The comprehensiveness and multidisciplinary nature of hybrid threats will require countries to change how they address national security. It will be necessary to revise strategies related to collaboration between authorities, collection of data, data fusion and analytics to create a holistic approach to security. In this way, hybrid threats will be a catalyst for updating and modernising modus operandi in the security domain.

2.7.5 Stakeholders

2.7.5.1 European Union stakeholders

European Commission Directorate-General for Internal Market, Industry, Entrepreneurship and SMEs

The mission of DG Internal Market, Industry, Entrepreneurship and SMEs is to develop a deeper and fairer internal market and help European enterprises, in particular start-ups and SMEs, and manufacturing and services industries to be globally competitive, innovative and sustainable, and to create more jobs, growth and value for all. The DG is a major contributor to two of the Commission's priorities: (1) a new boost for jobs, growth and investment and (2) a deeper and fairer internal market with a strengthened industrial base. DG Internal Market, Industry, Entrepreneurship and SMEs also significantly contributes to other two of the Commission's priorities: (3) a connected digital single market and (4) a resilient energy union with a forward-looking climate change policy. According to its strategic plan 2016-2020, the DG is working together with the EEAS to counter hybrid threats. The Commission aims to build resilience to potential hybrid threats and increase cooperation with international partners on the issue (European Commission, 2016b).

https://ec.europa.eu/growth/index_en

European Commission Directorate-General for Migration and Home Affairs

DG Migration and Home Affairs manages policies that aim to ensure that all activities necessary and beneficial to the economic, cultural and social growth of the EU can develop in a stable, lawful and secure environment. It aims to develop a balanced and comprehensive EU migration policy, based on solidarity and responsibility, building a safer Europe by fighting terrorism and organised crime, by promoting police cooperation and by preparing to respond swiftly to emerging crises.

DG Migration and Home Affairs, together with the JRC, develops tools and vulnerability indicators to address hybrid threats to critical infrastructures (Giannopoulos et al., 2018).

https://ec.europa.eu/home-affairs/index_en

European Commission Directorate-General Joint Research Centre

The JRC is the European Commission's science and knowledge service. It has solid research and policy support experience, developed in house, as well as broad networks with academia, industry, Member States and city authorities.

The JRC, thanks to its anticipatory thinking and its broad expertise in various fields related to hybrid threats, was among the first DGs to conduct work in this area. See Section 3.4 for more details.

https://ec.europa.eu/info/departments/joint-research-centre_en

European External Action Service

The EEAS is the EU's diplomatic service, which works closely with the foreign and defence ministries of the EU Member States and with EU institutions. It also has a strong working relationship with the UN and other international organisations. It helps the HR/VP to implement the EU's CFSP.

https://eeas.europa.eu/topics/security-defence-crisis-response/47517/implementing-global-strategy-eu-delivers-security-and-defence_en

The EU Hybrid Fusion Cell was established in 2016, within the existing EU Intelligence and Situation Centre, aiming to provide all-source analysis on hybrid threats. As envisaged in the joint framework on countering hybrid threats⁽¹²⁸⁾, it receives, analyses and shares classified and open-source information specifically relating to indicators and warnings concerning hybrid threats; the information comes from various stakeholders within the EEAS, the Commission (and the EU agencies) and Member States. In liaison with similar bodies at EU and national levels, the Fusion Cell deals with external aspects of hybrid threats affecting the EU and its neighbourhood, rapidly analysing relevant incidents and informing the EU's strategic decision-making processes, including by providing inputs into the security risk assessments carried out at EU level. Member States are expected to establish national contact points connected to the EU Hybrid Fusion Cell (EEAS, 2018).

Communication task forces for the EU's eastern and southern neighbourhoods have been established to counter widespread disinformation campaigns and systematic diffusion of fake news. The guidelines issued on the basis of the Council conclusions of March 2015 provided a mandate for establishing the EEAS East StratCom Task Force. In 2017, the EEAS decided to set up two forces, the EEAS StratCom Western Balkans Task Force and the EEAS StratCom South Task Force⁽¹²⁹⁾.

The East StratCom Task Force develops communication products and campaigns focused on better explaining EU policies in the Eastern Partnership countries (Armenia, Azerbaijan, Belarus, Georgia, Moldova and Ukraine). It supports EU efforts to strengthen the media environment in the Eastern Partnership region, in collaboration with other EU actors. The task force reports on and analyses disinformation trends, explains and corrects disinformation narratives, and raises awareness of disinformation. It works with the EU institutions, EU delegations in the Eastern Partnership countries, Member States and a wide range of other partners, both governmental and non-governmental, within the EU, in the eastern neighbourhood, and beyond. This international cooperation aims to share best practices in strategic communications and provide access to objective information, as well as ensuring support for independent media in the region⁽¹³⁰⁾.

European Defence Agency

The EDA is an intergovernmental agency of the Council of the European Union, to which it reports and from which it receives guidelines. It has three main missions: (1) supporting the development of defence capabilities and military cooperation among the EU Member States, (2) stimulating defence research and technology and strengthening the European defence industry and (3) acting as a military interface to EU policies.

One of the domains in which the EDA is active is cyber- and hybrid warfare. This work comprises several projects on topics such as cyberdefence, radiofrequency sensor technologies, information, optronics, governmental satellite communications, communications and information systems, persistent surveillance long-term analysis and hybrid warfare.

In 2016, the EDA organised the Hybrid Threats Table Top Exercise, with the participation of DG Internal Market, Industry, Entrepreneurship and SMEs, DG Energy, DG Mobility and Transport, DG Migration and Home Affairs, ECHO, the EEAS, CERT-EU, ENISA and Europol, as well as observers from NATO. The objective of the exercise was to identify and analyse the implications of hybrid threats for European military capability development⁽¹³¹⁾.

The EDA is currently managing the Consultation Forum for Sustainable Energy in the Defence and Security Sector⁽¹³²⁾, a European Commission initiative aimed at bringing together specialists from the defence and energy sectors to share data and best practices on, for example, energy efficiency, renewable energy, and the protection and resilience of critical infrastructures for defence energy. In October 2017, the final report on

⁽¹²⁸⁾ European Commission and High Representative joint communication JOIN(2016) 18 final.

⁽¹²⁹⁾ Estonian Presidency of the Council of the European Union, 'Estonian Foreign Minister Sven Mikser: EU must strengthen strategic communication capability' (<https://www.eu2017.ee/news/press-releases/estonian-foreign-minister-sven-mikser-eu-must-strengthen-strategic>).

⁽¹³⁰⁾ EEAS, 'Questions and answers about the East StratCom Task Force' (https://eeas.europa.eu/headquarters/headquarters-homepage/2116/questions-and-answers-about-east-stratcom-task-force_en).

⁽¹³¹⁾ EDA, 'Countering hybrid threats: EDA hosts first table top exercise' (<https://www.eda.europa.eu/info-hub/press-centre/latest-news/2016/03/11/countering-hybrid-threats-eda-hosts-first-table-top-exercise>).

⁽¹³²⁾ EDA, 'Consultation forum for sustainable energy in the defence and security sector (CF SEDSS)' (<https://www.eda.europa.eu/european-defence-energy-network>).

the first phase was released (EDA, 2017b) and the second phase was launched. This project has received funding from the H2020 research and innovation programme and the agreement is between the Executive Agency for Small and Medium-sized Enterprises and the EDA, with support from the JRC.

<https://www.eda.europa.eu/what-we-do/activities>

European Union Agency for Law Enforcement Cooperation (Europol)

Europol is the EU's law enforcement agency. It supports the EU Member States in their fight against terrorism, cybercrime and other serious and organised forms of crime. It also works with many non-EU partner states and international organisations.

The EU IRU was set up by the Justice and Home Affairs Council of the EU and is built upon Europol's Check-the-Web service. Its main role is to anticipate and pre-empt terrorist abuse of online tools, as well as to play a proactive advisory role in relation to EU Member States and the private sector in this regard.

A key unit of Europol's ECTC, EU IRU focuses on:

- supporting the competent EU authorities by providing strategic and operational analysis;
- flagging terrorist and violent extremist online content and sharing it with relevant partners;
- detecting and requesting the removal of internet content used by smuggling networks to attract migrants and refugees;
- swiftly carrying out and supporting the referral process, in close cooperation with the industry.

The EU IRU's tactical approach to referrals is targeted. The procedure aims to focus on propaganda linked to a high-profile event (e.g. the Paris attacks, the Brussels attack, the Magnanville murder) and relayed by high-profile accounts. The primary objective is to be effective during the 'viral' phase of the propaganda. The secondary objective is to gather information to better understand the tactics and *modi operandi* of the main online propagandists, in order to improve the disruption mechanism.

In addition to providing support to the EU Member States, EU IRU cooperates with third-party partners within the framework of the EU Internet Forum. In this context and with the European Commission's support, EU IRU has engaged with online service companies to promote self-regulation activities by the online industry ⁽¹³³⁾.

<https://www.europol.europa.eu/about-europol>

2.7.5.2 International stakeholders

North Atlantic Treaty Organization

NATO's Joint Intelligence and Security Division, Hybrid Analysis Branch, was established in July 2017. Its mandate is to analyse the full spectrum of hybrid actions, drawing from military and civilian, classified and open sources ⁽¹³⁴⁾.

In addition, two CoE contribute to NATO's efforts to counter hybrid threats: the Strategic Communications CoE in Riga, Latvia, and the Cooperative Cyber Defence CoE in Tallinn, Estonia. Both organisations are international research centres that are nationally or multinationally funded and staffed. They work alongside and contribute knowledge and expertise to the alliance, but they are not NATO bodies.

On 8 July 2016, a joint declaration on EU–NATO partnership was signed by the President of the European Council, the President of the European Commission and the Secretary-General of NATO ⁽¹³⁵⁾. It identifies seven areas of cooperation: countering hybrid threats; operational cooperation, including at sea and on migration, cybersecurity and defence; defence capabilities; defence industry and research; exercises; and supporting eastern and southern partners' capacity-building efforts. In total, 74 specific actions are under implementation in the 7 areas; 20 of them centre on countering hybrid threats. Interaction between the EU Hybrid Fusion Cell and the NATO Hybrid Analysis Branch is an important element of EU–NATO cooperation on hybrid threats.

⁽¹³³⁾ Europol, 'Europol Internet Referral Unit one year on' (<https://www.europol.europa.eu/newsroom/news/europol-internet-referral-unit-one-year>).

⁽¹³⁴⁾ NATO, 'Adapting NATO intelligence in support of "one NATO" ' (<https://www.nato.int/docu/review/2017/Also-in-2017/adapting-nato-intelligence-in-support-of-one-nato-security-military-terrorism/EN/index.htm>).

⁽¹³⁵⁾ EEAS, 'EU–NATO cooperation — factsheets' (https://eeas.europa.eu/headquarters/headquarters-homepage/28286/eu-nato-cooperation-factsheet_en).

An EU operational protocol, the EU Playbook, has been developed; it outlines practical arrangements for coordination, intelligence collation, analysis and cooperation with partner organisations, including NATO ⁽¹³⁶⁾. It was tested in the 2017 Parallel and Coordinated Exercise and further tested in the 2018 exercise.

<https://www.nato.int/>

European Centre of Excellence for Countering Hybrid Threats

Hybrid CoE was established in 2017 to serve as a hub of expertise supporting the participating countries' individual and collective efforts to enhance their civil-military capabilities, resilience and preparedness to counter hybrid threats with a special focus on European security. Participation in the centre is open to EU Member States and NATO allies. Currently, the participants are Estonia, Finland, France, Germany, Latvia, Lithuania, the Netherlands, Norway, Poland, Spain, Sweden, the United Kingdom and the United States. The aim of Hybrid CoE is to provide a single location dedicated to furthering a common understanding of hybrid threats at a strategic level and promoting the development of comprehensive, whole-of-government responses at national levels and of coordinated responses at EU and NATO levels. In addressing these issues, the functions of Hybrid CoE include the following:

- to encourage strategic-level dialogue and consultation between and among participants, the EU and NATO;
- to conduct research and analysis into hybrid threats and methods to counter them;
- to develop doctrine, conduct training and arrange exercises aimed at enhancing the participants' individual capabilities, as well as interoperability between and among participants, the EU and NATO to counter hybrid threats;
- to engage with and invite dialogue with governmental and non-governmental experts from a wide range of professional sectors and disciplines;
- to involve, or cooperate with, communities of interest, focusing on specific activities that may constitute hybrid threats, on methodologies for understanding these activities and on ways to adjust organisations to better address threats effectively.

<https://www.hybridcoe.fi>

2.7.6 Legislation and reference documents

- European Commission, Commission communication, 'The European agenda on security' (COM(2015) 185 final), Strasbourg, 28 April 2015.
- European Commission and High Representative of the Union for Foreign Affairs and Security Policy, joint communication, 'Joint framework on countering hybrid threats: a European Union response' (JOIN(2016) 18 final), Brussels, 6 April 2016.
- European Commission, Commission communication, 'Delivering on the European agenda on security to fight against terrorism and pave the way towards an effective and genuine security union' (COM(2016) 230 final), Brussels, 20 April 2016.
- European Commission and High Representative of the Union for Foreign Affairs and Security Policy, joint staff working document, 'EU operational protocol for countering hybrid threats: "EU Playbook"' (SWD(2016) 227 final), Brussels, 5 July 2016.
- European Commission, 'Reflection paper on the future of European defence' (COM(2017) 315 final), Brussels, 7 June 2017.
- European Commission and High Representative of the Union for Foreign Affairs and Security Policy, joint report, *The implementation of the Joint Framework on countering hybrid threats — A European Union response* (JOIN(2017) 30 final), Brussels, 19 July 2017.
- European Commission and High Representative of the Union for Foreign Affairs and Security Policy, joint report, *The implementation of the Joint Framework on countering hybrid threats from July 2017 to June 2018* (JOIN(2018) 14 final), Brussels, 13 June 2018.

⁽¹³⁶⁾ European Commission and High Representative for Foreign Affairs and Security Policy, joint staff working document, 'EU operational protocol for countering hybrid threats: "EU Playbook"' (SWD(2016) 227 final), Brussels, 5.7.2016.

— European Parliament, European Council and Council, joint communication, 'Increasing resilience and bolstering capabilities to address hybrid threats' (JOIN(2018) 16 final), Brussels, 13 June 2018.

2.8 Combating radicalisation to terrorism

2.8.1 The European Union's rationale for focusing on eradicating terrorism at its source — the why and what

The EU has suffered many deaths resulting from terrorist attacks in the past two decades: Madrid (2004), London (2005), Paris (2015), Brussels (2016), Nice (2016), Berlin (2016), London (2017), Barcelona (2017) and Strasbourg (2018). This has strengthened the need to address radicalisation leading potentially to violent extremism and terrorism. The eradication of terrorism starts at the source; therefore, a priority of the EU internal security strategy in action (Council of the European Union, 2015) is combating radicalisation and recruitment to terrorism.

Radicalisation is a process whereby an individual's or group's thoughts and beliefs (ideological, religious or political) deviate from what society accepts as norms. In other words, it is a process whereby people shift towards extremism⁽¹³⁷⁾. Academic models depict radicalisation as a gradual, complex, dynamic and multifaceted evolution of interconnected and recurring factors over a period of time.

This shifting process of interior and personal change can trigger actions geared towards ideological, political or social change and, in most cases, these are peaceful and do not necessarily result in serious harm. Only a few of those who are radicalised turn to terrorism. However, in exceptional circumstances, when the shift in behaviour leads to an explicit decision to use fear, terror or violence to achieve change, the result is violent extremism⁽¹³⁸⁾. Terrorism is a type of violent extremism, like xenophobia or other forms of discrimination (UN Security Council, 2015).

Recruitment, radicalisation and incitement to terrorism can be visualised as points along a continuum. Radicalisation can be interpreted as the indoctrination process of transforming potential recruits or recruits into individuals determined to act with violence. The radicalisation process often involves use of propaganda, whether communicated in person or over the internet, over time. The length of time and the effectiveness of the propaganda and other persuasive means employed depend on individual circumstances and relationships (UNODC, 2016).

Recent observations made by the Radicalisation Awareness Network (Radicalisation Awareness Network, 2017) show that violent extremist groups can grow out of religious extremism or left wing, right wing, anarchist, nationalist or separatist ideologies. Furthermore, violent extremists can be part of hierarchical organisations, members of smaller cells and or 'lone wolves'. Consequently, terrorist or violent extremist actions are challenging for the authorities to detect and predict, making traditional law enforcement techniques alone insufficient to deal with these evolving trends, particularly in relation to tackling the root causes of the problem. A wider, systemic and participatory multistakeholder approach is needed to enable the timely identification of causes, pathways and interconnections for effective management.

The EU has prioritised the need to govern terrorism pre-emptively by investing in and implementing a counterterrorism strategy with a robust but flexible design (see Section 2.8.3).

2.8.2 How do terrorists recruit and operate?

Radicalisation and recruitment of new members of terrorist groups are now most commonly carried out using the internet and social media. It seems to be the case that people who are hooked by online means to a terrorist cause have been explicitly targeted (Alarid, 2016). These radicalised people are not necessarily religious; for example, Muslims radicalised online are not necessarily devout and are demographically varied, ranging from poorly to highly educated, with no common factor in terms of country of origin, gender, age or financial status. Their vulnerability seems sometimes to lie in the fact that they feel there is something missing from their lives, while they are also living in a climate of inequality and political frustration (Alarid, 2016).

⁽¹³⁷⁾ The word 'extremism' is, however, to be used with great caution as mentioned by Neumann (2017, p. 16), who states that 'the meaning of extremism depends on what is seen as "mainstream" in any given society, section of society, or period of time. Different political, cultural and historical contexts produce different notions of extremism.'

⁽¹³⁸⁾ Australian Government, 'Living safe together: building community resilience to violent extremism — resources' (<https://www.livingsafetogether.gov.au/information/Pages/resources.aspx>).

Drivers of violent extremism are complex, multifaceted and interconnected, and are particular to the structural environment in which radicalisation and possibly violent extremism can start to burgeon (UNDP, 2016; Miller and Selig Chauhan, 2017). Examples of drivers could be severe alienation, perceived injustice or humiliation reinforced by social marginalisation, xenophobia and discrimination, limited education or employment possibilities, criminality, political factors combined with an ideological and religious dimension, unstructured family ties, personal trauma and other psychological problems ⁽¹³⁹⁾. Vulnerable people (women, children, prisoners, refugees, etc.) in such conditions are prone to being exploited by terrorist (religious or ideological) recruiters.

Members of such vulnerable groups are targeted using manipulative information composed of both truths and lies, provided in a narrative that has been created ad hoc to influence thoughts and attitudes, with a view to encouraging people to behave in a particular manner. Some authors offer an analysis of the structure of recruitment processes that use effective, specific pitches, geared to the target individual or group (Gerwehr and Daly, 2006). The recruiter fine-tunes the customised pitch based on psychological attributes (personality, values, opinions, attitudes, interests, lifestyle, environment, etc.). What has been observed, on the one hand, is that there is no unique standard recruitment mode, that is, recruitment processes vary according to distinct locations (nodes), such as prisons, schools, etc., by region (geographical location) and depending on the specific characteristics (closed or open, local culture, etc.) of the context in which the recruitment group is operating. Processes vary over time and based on the situation. On the other hand, there is no one-size-fits-all counter-recruitment approach to mitigate or prevent terrorist recruitment; counter-recruitment intervention design must be adjusted ad hoc to the particular characteristics of the target audience.

The same authors also offer a non-exhaustive list of four examples of recruitment structures (based on patterns and descriptors characterising terrorist groups' recruitment behaviour) used by Al-Qaeda to which counter-recruitment measures need to be adapted:

- net — used for a specific population that is deemed homogeneous enough to be targeted in its entirety (i.e. one pitch for all);
- funnel — used when a target population requires an incremental or phased approach to transform the identity and increase the motivation of potential recruits with the help of group identity-building exercises, violence, etc., resulting in the desired radically polarised and altered attitudes;
- infection — used for a specific population that is deemed insular and a challenge to reach, with a trusted recruiting agent inserted to rally potential recruits in a more direct and ad hoc manner;
- seed crystal — used for a specific population that is remote and inaccessible, for which trusted agents cannot be used and over which a media net cannot be cast, with recruiters therefore carefully designing a context for self-recruitment.

Miller and Selig Chauhan (2017) examine explanatory models for the radicalisation process, the majority of which tend to describe similar sequential steps that lead 'away from a state of apparent normalcy and toward a state of violent radicalism'. This is a process that starts with ideological engagement, shifts to radicalisation, moves next to a catalyst event and finally results in violent extremism or terrorism.

Gøtzsche-Astrup (2018) classifies and evaluates radicalisation mechanisms based on empirical evidence. He presents six approaches ⁽¹⁴⁰⁾ to psychological radicalisation, based on an in-depth literature review. He explains that it is of the utmost importance to understand radicalisation psychology and that it has become an empirical endeavour, where researcher-practitioner collaborations could lead to advances in this research field. He looks at the causes of radicalisation in the different models and claims that they have a common core, although conflicting claims may be made about radicalisation causes.

These are all different ways looking at how terrorists (ideological or religious) may operate. They can all help us to better understand the complex mechanisms related to the radicalisation phenomenon and to design better counter-radicalisation strategies and action plans.

⁽¹³⁹⁾ European Commission, Commission communication, 'Supporting the prevention of radicalisation leading to violent extremism' (COM(2016) 379 final), Brussels, 14.6.2016.

⁽¹⁴⁰⁾ The six approaches are uncertainty-identity theory (Hogg and Adelman, 2013), significance quest / '3N' (Webber and Kruglanski, 2018), the devoted actor model (Atran, 2016), mindset and worldview (Borum, 2014), reactive approach motivation (McGregor, et al., 2015) and the two-pyramids approach (McCauley and Moskaleiko, 2017) (see pp.91-96 of paper for more details).

2.8.3 The European Union's strategy for combating radicalisation and recruitment to terrorism

Responsibility for fighting against violent radicalisation leading to terrorism is mainly a national matter; however, because of the transboundary nature of the issue, the EU provides a framework to help in coordinating national policies, sharing information and determining good practice. In 2005, the Council of the European Union established an EU counterterrorism strategy (Council of the European Union, 2005a) to fight terrorism globally and make Europe safer. The strategy focused on four pillars: prevent, protect, pursue and respond. The first pillar established 'addressing the causes of radicalisation and terrorism recruitment' as a key priority for the EU. To this end, the Council adopted in 2005 an EU strategy for combating radicalisation and recruitment to terrorism (Council of the European Union, 2005b). This strategy was revised in 2008 and 2014 (Council of the European Union, 2008, 2014c), on the second occasion to take into consideration evolving threats such as lone-actor terrorism, foreign fighters and the use of social media by terrorists.

In December 2014, the Council agreed on a set of guidelines to complement the revised EU strategy on radicalisation (Council of the European Union, 2014d). These guidelines were reviewed and updated in 2017 (Council of the European Union, 2017b), taking into account the evolution of threats.

For its part, the European Commission released in 2005 a communication on terrorist recruitment addressing the factors contributing to violent radicalisation⁽¹⁴¹⁾. It identified priorities for action, with a focus on areas such as, broadcast media, the internet, education, youth engagement, employment, social exclusion and integration issues, equal opportunities and non-discrimination, and intercultural dialogue, among others.

The evolution of trends in, means of and patterns of radicalisation led the Commission to adopt in 2014 a new communication on strengthening the EU's response⁽¹⁴²⁾. In 2015, the European agenda on security⁽¹⁴³⁾ put the prevention of violent radicalisation in a broader policy context, making tackling terrorism and preventing radicalisation one of its three priorities (together with disrupting organised crime and combating cybercrime).

In 2016, the Commission updated its actions to support the prevention of radicalisation in a new communication⁽¹⁴⁴⁾, which focused on how work at EU level can support Member States in facing the radicalisation challenge. It identified seven areas for action:

1. countering terrorist propaganda and illegal hate speech online;
2. addressing radicalisation in prisons;
3. promoting inclusive education and EU common values;
4. promoting an inclusive, open and resilient society and reaching out to young people;
5. strengthening international cooperation: the EU will assist non-EU countries facing similar challenges in addressing radicalisation through law enforcement and human rights-compliant responses;
6. boosting research, evidence building, monitoring and networks by producing concrete tools and policy analysis to better understand the process of radicalisation, to be directly usable by Member States' security practitioners and policymakers, building also on the work of the Radicalisation Awareness Network Centre of Excellence;
7. focusing on the security dimension — prevention of radicalisation also requires a core security approach involving measures to counter immediate and longer-term threats — such as travel prohibitions and the criminalisation of travelling to non-EU countries for terrorist purposes, as already proposed by the Commission —and actions by Member States including increased information sharing, making full use of security cooperation frameworks and information tools, and reinforcing the interconnection of information systems.

In 2011, the Commission established the Radicalisation Awareness Network⁽¹⁴⁵⁾, an EU network connecting key organisations and networks of local actors involved in preventing radicalisation to terrorism and violent

⁽¹⁴¹⁾ European Commission, Commission communication, 'Concerning terrorist recruitment: addressing the factors contributing to violent radicalisation' (COM(2005) 313 final), Brussels, 21.9.2005.

⁽¹⁴²⁾ European Commission, Commission communication, 'Preventing radicalisation to terrorism and violent extremism: strengthening the EU's response' (COM(2013) 941 final), Brussels, 15.1.2014.

⁽¹⁴³⁾ European Commission communication COM(2015) 185 final.

⁽¹⁴⁴⁾ European Commission communication COM(2016) 379 final.

⁽¹⁴⁵⁾ https://ec.europa.eu/home-affairs/what-we-do/networks/radicalisation_awareness_network

extremism, including first-line practitioners and field experts such as social and health workers, teachers, civil society organisations, local authorities, law enforcement officers, security officials, counterterrorism specialists, think tanks, institutes and academics. Moreover, in 2015, the Commission set up the EU Internet Forum to tackle the problem of online radicalisation.

Continuing with its work, in July 2017 the Commission set up the High-Level Expert Group on Radicalisation⁽¹⁴⁶⁾, tasked with offering advice on (i) ways to improve cooperation among stakeholders and Member States, (ii) the further development of policies for the prevention of radicalisation and (iii) a mechanism for future structured cooperation in this area. In May 2018, the group released its final report (High-Level Expert Group on Radicalisation, 2018) presenting a number of recommendations to the Commission to address challenges in the following areas:

- radicalisation in prisons;
- online propaganda and communication;
- ideology and polarisation;
- cooperation at local level;
- education and social inclusion;
- children returning from conflict zones or raised in a radicalised environment.

In addition, the European Commission:

- supports research and studies to better understand the radicalisation process, its key influencing factors, ideologies and recruitment mechanisms (e.g. to inform methods used to counter the dissemination of terrorist propaganda, especially on the internet);
- has established a European Network of Experts on Radicalisation to provide an arena to discuss the radicalisation phenomenon and to assist EU and national-level policymakers in gathering expertise and identifying and exchanging good practices in the field of prevention;
- promotes public-private partnerships and dialogue between law enforcement authorities and internet service providers to reduce terrorism-related and other illegal content on the internet;
- enhances law enforcement authorities' technical resources and know-how on tools and methodologies that detect illegal content online;
- provides assistance to governmental and non-governmental stakeholders in developing EU-wide cooperation and actions to strengthen individual and community resilience against radicalisation under the prevention of and fight against crime programme⁽¹⁴⁷⁾.

To complement the abovementioned activities, the EU continues to focus on actions related to education, youth participation, and interfaith and intercultural dialogue, as well as employment and social inclusion⁽¹⁴⁸⁾. The Commission is focusing its efforts particularly on the younger generation, by combating youth radicalisation and marginalisation, as evidenced by a series of targeted actions under the following initiatives: the strategic framework for European cooperation on education and training⁽¹⁴⁹⁾, the European youth strategy⁽¹⁵⁰⁾, and the EU work plan for sport and culture (Council of the European Union, 2017c). Finally, with the aim of underpinning these actions, the Commission provides funding under the Erasmus+ and Creative Europe programmes⁽¹⁵¹⁾, as well as through the European Social Fund⁽¹⁵²⁾.

⁽¹⁴⁶⁾ European Commission, Commission decision setting-up the high-level commission expert group on radicalisation (C(2017) 5149 final), Brussels, 27.7.2017.

⁽¹⁴⁷⁾ European Commission, 'Prevention of and fight against crime (ISEC)' (<https://ec.europa.eu/home-affairs/financing/fundings/security-and-safeguarding-liberties/prevention-of-and-fight-against-crime>).

⁽¹⁴⁸⁾ See European Union, 'From awareness to prevention: how the EU is combating radicalisation across Europe' (https://europa.eu/euprotects/our-safety/awareness-prevention-how-eu-combating-radicalisation-across-europe_en).

⁽¹⁴⁹⁾ Council of the European Union, Council conclusions on a strategic framework for European cooperation in education and training ('ET 2020') (2009/C 119/02), Brussels, 12.5.2009.

⁽¹⁵⁰⁾ European Commission, 'EU youth strategy' (https://ec.europa.eu/youth/policy/youth-strategy_en).

⁽¹⁵¹⁾ These programmes support the mobility of teachers and youth workers; they promote youth exchanges and volunteering, strategic partnerships in the education and youth policy areas, transnational networks, school cooperation platforms, joint projects on citizenship education and collaborative partnerships in sport.

⁽¹⁵²⁾ The fund provides financial assistance to Member States by promoting social inclusion and combating poverty and discrimination.

2.8.4 Possible evolution of radicalisation within the next 5 years

In the past decade, the concept of radicalisation has changed; these changes have been driven by the Syrian war and the rise of far-right nationalist parties in Europe, which have reshaped how political violence is analysed and explained. Greater attention has been paid to the resilience of society to extremist narratives and recruitment attempts. For this reason, experts advise further research on narrative commonalities between far-right and Islamist groups, in order to understand how these messages are constructed to appeal to a relatively large audience (Rieger et al., 2013). Differences in political cultures, ideologies, legal frameworks and religions need to be taken in consideration to avoid proposing a one-size-fits-all type of solution. Challenges may also come from terrorist recidivism, about which there are still not enough data to assess whether or not deradicalisation programmes have been successful (Koehler, 2016). Various experts have identified a number of near-future challenges:

- the return of foreign fighters from Syria, Iraq and Libya;
- travelling extremist preachers ⁽¹⁵³⁾;
- internet propaganda (Ahmed and Lloyd George, 2017);
- extremist content on satellite TV;
- radicalisation of second- and third-generation migrants as a result of failure to include them in society (Roy, 2016);
- culture shock experienced by non-integrated first-generation migrants;
- an increase in violent and hate speech by far-right groups.

2.8.5 Stakeholders

2.8.5.1 European Union stakeholders

European Commission Directorate-General for Migration and Home Affairs

DG Migration and Home Affairs is responsible for policymaking in the area of migration and security. It deals with dialogue and cooperation with countries outside the EU and assists in raising awareness among EU citizens of these important topics.

In the effort to combat radicalisation, the Commission's role is to support Member States. DG Migration and Home Affairs has a dedicated service, Unit D.2, Terrorism and Radicalisation, that deals with this complex, multidisciplinary and challenging task. In this endeavour, it cooperates with other units: Police Cooperation and Information Exchange (D.1), Organised Crime and Drugs Policy (D.3), Cybercrime (D.4), Information Systems for Borders and Security (B.3), and Innovation and Industry (B.4). Through DG Migration and Home Affairs' Directorate E (Migration and Security Funds — Financial Resources and Monitoring), funding is provided to projects addressing this topic.

https://ec.europa.eu/home-affairs/what-we-do/policies/crisis-and-terrorism/radicalisation_en

Radicalisation Awareness Network

Established in 2011, the Radicalisation Awareness Network is an EU network of front-line or grass-roots practitioners (5 000 in 2018) from around Europe who work daily with people who have already been radicalised or who are vulnerable to radicalisation. Practitioners include police and prison authorities but also those who are not traditionally involved in counterterrorism activities, such as teachers, youth workers, civil society representatives, local authority representatives and healthcare professionals.

The activities of the network are carried out within nine working groups: Communication and Narratives; Education; EXIT; Youth, Families and Communities; Local Authorities; Prison and Probation; Police and Law Enforcement; Terrorism Victims Remembrance; and Health and Social Care.

https://ec.europa.eu/home-affairs/what-we-do/networks/radicalisation_awareness_network

⁽¹⁵³⁾ DW.COM, 'Gulf States supporting ultraconservative Islam branch in Germany' (<https://www.dw.com/en/reports-gulf-states-supporting-ultraconservative-islam-branch-in-germany/a-36746943>).

European External Action Service

The EEAS is the EU's diplomatic service, which works closely with the foreign and defence ministries of the EU Member States and with EU institutions. It also has a strong working relationship with the UN and other international organisations. It helps the HR/VP to implement the EU's CFSP.

<https://eeas.europa.eu/>

European Union Agency for Law Enforcement Cooperation (Europol)

Europol is the EU's law enforcement agency and assists the Member States in their fight against serious international crime and terrorism. Established as an EU agency in 2009, Europol is at the heart of the European security architecture and offers a unique range of services. Europol is a support centre for law enforcement operations, a hub for information on criminal activities and a centre for law enforcement expertise.

In January 2016, Europol established the ECTC, an operations centre and hub of expertise that reflects the growing need for the EU to strengthen its response to terror. The ECTC focuses on the following activities:

- providing operational support for investigations upon request from an EU Member State;
- tackling foreign fighters;
- sharing intelligence and expertise on terrorism financing (through the Terrorist Finance Tracking Program (TFTP) and financial intelligence units);
- combating online terrorist propaganda and extremism (through the EU IRU);
- fighting against illegal arms trafficking;
- international cooperation among counterterrorism authorities.

<https://www.europol.europa.eu/about-europol/european-counter-terrorism-centre-ectc>

European Union Institute for Security Studies (EUISS)

The EUISS is the EU agency dealing with the analysis of foreign, security and defence policy issues. It was established in January 2002 as an autonomous agency under the CFSP to foster a common security culture for the EU, support the creation and implementation of its foreign policy, and enrich the strategic debate inside and outside Europe. Its core mission is to provide analyses and fora for discussion that can be of use and relevance for the formulation of EU policy. In carrying out that mission, it also acts as an interface between European experts and decision-makers at all levels.

<https://www.iss.europa.eu/>

2.8.5.2 International stakeholders

United Nations Office on Drugs and Crime (UNODC)

UNODC is a world leader in the fight against illicit drugs and international crime. It has a mandate to help Member States in addressing illicit drugs, crime and terrorism. It is supported by three pillars: field-based technical cooperation projects to build the capacity of Member States to counter illicit drugs, crime and terrorism; research and analytical work to build the knowledge base required for evidence-based policy support and operational decision making; and normative work to assist Member States in ratifying and implementing international treaties, developing national legislation, etc. Its work includes collaborating with partners on radicalisation issues in many countries.

An example of such work is UNODC's efforts to manage violent extremist prisoners and to prevent radicalisation, on which it has produced a handbook (UNODC, 2016).

<https://www.unodc.org/unodc/en/terrorism/index.html>

Organisation for Economic Co-operation and Development

The OECD promotes policies that aim to improve the economic and social well-being of people around the world. It draws on facts and real-life experience to focus on helping governments to restore confidence in markets and the institutions that make them function; re-establishing healthy public finances as a basis for future sustainable economic growth; fostering and supporting new sources of growth through innovation,

environmentally friendly 'green growth' strategies and the development of emerging economies; and ensuring that people of all ages can develop the skills to work productively and satisfyingly in the jobs of tomorrow.

<http://www.oecd.org/social/understanding-the-battle-against-extremism.htm>

United Nations Development Programme (UNDP)

UNDP builds on its strength and expertise, country relationships and presence on the ground in more than 170 countries and territories. It works to strengthen international cooperation on developmental and economic issues. It connects countries around the globe to knowledge, experience and resources that can help them overcome a variety of challenges in the developmental realm. It helps people build a better life. It provides expert advice, training and grants to developing countries, with an increasing emphasis on assistance to the least developed countries.

One of its recent reports addressed radicalisation and violent extremism from a development perspective (UNDP, 2016). It looks at drivers of violent extremism, describes pathways from radicalisation to violent extremism, and attempts to identify where the tipping point is in the process. It also presents building blocks for preventing violent extremism.

www.undp.org

2.8.6 Legislation and reference documents

- European Commission, Commission communication, Preparedness and consequence management in the fight against terrorism (COM(2004) 701 final), Brussels, 20 October 2004.
- European Commission, Commission communication, 'Concerning terrorist recruitment: addressing the factors contributing to violent radicalisation' (COM(2005) 313 final), Brussels, 21 September 2005.
- Council of the European Union, *The European Union Counter-Terrorism Strategy* (14469/4/05), Brussels, 30 November 2005.
- Council Decision 2007/124/EC, Euratom, of 12 February 2007 establishing for the period 2007 to 2013, as part of General Programme on Security and Safeguarding Liberties, the Specific Programme 'Prevention, Preparedness and Consequence Management of Terrorism and other Security-related risks', OJ L 58, 24.2.2007, p. 1-6.
- European Commission, Commission communication, 'Stepping up the fight against terrorism' (COM(2007) 649 final), Brussels, 6 November 2007.
- European Commission, Commission communication, 'The EU counter-terrorism policy: main achievements and future challenges' (COM(2010) 386 final), Brussels, 20 July 2010.
- European Commission, Commission communication, 'Preventing radicalisation to terrorism and violent extremism: strengthening the EU's response' (COM(2013) 941 final), Brussels, 15 January 2014.
- Council of the European Union, *Revised EU strategy for combating radicalisation and recruitment to terrorism* (9956/14), Brussels, 19 May 2014.
- European Commission, Commission communication, 'The European agenda on security' (COM(2015) 185 final), Strasbourg, 28 April 2015.
- European Commission, Commission communication, 'Delivering on the European agenda on security to fight against terrorism and pave the way towards an effective and genuine security union' (COM(2016) 230 final), Brussels, 20 April 2016.
- European Commission, Commission communication, 'Supporting the prevention of radicalisation leading to violent extremism' (COM(2016) 379 final), Brussels, 14 June 2016.
- Council of the European Union, *Review of the guidelines for the EU strategy for combating radicalisation and recruitment to terrorism* (6700/17), Brussels, 9 March 2017.
- Directive (EU) 2017/541 of the European Parliament and of the Council of 15 March 2017 on combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA, OJ L 88, 31.3.2017, p. 6-21.

- European Commission, 'Reflection paper on the future of European defence' (COM(2017) 315 final), Brussels, 7 June 2017.
- Europol, *European Union (EU) serious and organised crime threat assessment — Crime in the age of technology*, 2017.
- Europol (2017), *European Union Terrorism Situation and Trend Report*, 2017.

2.9 Fighting against terrorism financing

2.9.1 The European Union's rationale for focusing on combating terrorism financing — the why and the what

The EU continues to carry out its efforts and meet its responsibility to sustain the Pax Europaea⁽¹⁵⁴⁾; however, the continuously evolving security risk landscape is very challenging owing to its complexity and unpredictability. Among these security risks is terrorism.

In the EU⁽¹⁵⁵⁾, terrorism financing is defined as 'the provision or collection of funds, by any means, directly or indirectly, with the intention that they should be used or in the knowledge that they are to be used, in full or in part, to carry out any of the offences defined in Framework Decision 2002/475/JHA'.

In the quest to use violence and intimidation, terrorists (individuals and organisations) require funds to ensure that their networks flourish, their ideology is promoted, recruitment and training continue, supply flows are maintained and planned terrorist acts put into action. They are very creative and adaptive in obtaining financing for their activities, constantly evolving in their efforts to seek, gather and mobilise funds. Thus, 'terrorism financing' refers to all activities related to the funding of terrorist acts.

These funding activities can be carried out using legitimate sources: self-financing (own salary), diaspora funds (personal donations, profits from businesses, etc.), donations from religious organisations or social or charitable organisations, or government sponsorships.

On the other hand, terrorism can also be financed from proceeds gained from traditional criminal sources (Napoleoni, 2005; USDOS, 2005; Freeman, 2011; Clunan, 2013; Bloemkolk, 2015; FATF, 2015a,b; Oftedal, 2015; Aliu et al., 2017): misuse of legal financial systems (credit card and cheque fraud), narcotics trafficking, precious stones trafficking, arms trafficking, human trafficking, racketeering (extortion), counterfeiting, smuggling, and abduction and ransom demands.

Terrorist groups tend to also use front companies, that is, commercial enterprises that engage in legal activities, with illicit money mixing with legitimate profits. This is where terrorists use money laundering techniques pioneered by very experienced transnational organised crime groups.

Against this background, the Heads of State and Government of the seven most industrialised nations and Russia agreed at the Ottawa G8 Ministerial Meeting in December 1995 to 'pursue measures aimed at depriving terrorists of their sources of finance'⁽¹⁵⁶⁾. This initiative triggered the development of a series of subsequent events that contributed to building momentum towards an understanding of the importance of tackling terrorism financing at the global level. The first event was the adoption of a UN resolution outlining measures to eliminate international terrorism (UN, 1996). In 1999, the International Convention for the Suppression of the Financing of Terrorism was adopted by the UN General Assembly (UN, 1999). In 2001, in the aftermath of the 11 September attacks in New York, the Financial Action Task Force (FATF), initially established at the Paris G7 summit in 1989 to tackle money laundering in the drug trafficking scene, started to include combating terrorism financing as part of its mission⁽¹⁵⁷⁾.

The attacks of 11 September 2001 and the subsequent adoption of stringent anti-terrorism laws and regulations in the United States triggered two key focus-shifting phenomena (Napoleoni, 2005):

⁽¹⁵⁴⁾ This is the name given to the period of relative peace experienced by Europe following the Second World War, often associated above all with the creation of the EU and its predecessors; see, for example, The Nobel Prize, 'European Union (EU) — Nobel lecture' (<https://www.nobelprize.org/prizes/peace/2012/eu/26124-european-union-eu-nobel-lecture-2012/>).

⁽¹⁵⁵⁾ Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC, OJ L 141, 5.6.2015, p. 73–117.

⁽¹⁵⁶⁾ <http://www.g8.utoronto.ca/terrorism/terror96.htm>

⁽¹⁵⁷⁾ FATF, 'History of the FATF' (<http://www.fatf-gafi.org/about/historyofthefatf/>).

1. terrorist groups transferred their money laundering activities from the United States to Europe;
2. financiers withdrew terrorism capital from the United States and moved it to Europe.

These phenomena, accompanied by the occurrence of several terrorist acts (e.g. in Madrid in 2004 and in London in 2005), resulted in the EU stepping up its efforts to and investments in combating terrorism financing (Wesseling, 2013), which became a key initiative within the EU security agenda ⁽¹⁵⁸⁾. Cutting off key financial sources was intended to cripple terrorists' funding mechanisms. The EU has taken note of the FATF recommendations of 2012. Several are explicitly intended to target terrorism financing: Recommendation 5 (criminalisation of terrorism financing), Recommendation 6 (targeted financial sanctions related to terrorism and its financing), Recommendation 7 ⁽¹⁵⁹⁾ (financial sanctions related to proliferation) and Recommendation 8 (preventing the misuse of non-profit organisations).

2.9.2 How does terrorism financing work?

There are many types of terrorist organisations ⁽¹⁶⁰⁾. They can range from small (e.g. Indian Mujahedin, Harakat-ul Jihad Islami), large regional organisations (e.g. ISIL) or global entities (e.g. Al-Qaeda). In recent years, ISIL has garnered attention for its particularly ruthless attacks and its unique funding streams (bank robbery, pirating oil fields and robbing other economic assets).

Most terrorist organisations perform terrorist acts that are relatively low-cost given the damage they can inflict. In fact, the main terrorist attacks in the EU have cost less than EUR 22 000 ⁽¹⁶¹⁾. Furthermore, a study of how Jihadi terrorist cells in western Europe raise, move and spend money found that 90 % of the cells investigated were involved in income-generating activities, half of which were entirely self-financed (Ofsted, 2015). Thus, the current terrorist threat to Europe seldom involves huge sums of money or suspicious international transfers (Ofsted, 2015; European Parliament, 2018a).

What are costly are the operational costs of sustaining terrorist organisations. They have diverse revenue streams, legal and illegal. There is not much difference between terrorists and other criminals in their abuse of the financial system. While terrorism funding is different from money laundering, terrorists often exploit similar weaknesses in the financial system. Regardless of how they raise their capital, terrorist cells use several methods to 'clean' their money with the ultimate objective of disguising the origin of their funds by exploiting global financial networks, the illicit commodity trade, charities, attorneys or informal funds transfer systems, and cash couriers to launder money (USDOS, 2005).

According to a European Parliament study (2018b), terrorism financing can take several forms, such as:

- raising funds, for example through donations or criminal activity;
- moving funds, for example by transferring funds through banks from Europe to countries near theatres of combat or simply by carrying cash;
- storing funds, for example by maintaining reserves of cash that can later be spent on attacks, military operations, travel or other facilitation activities.

The six most widely used methods that terrorists groups use to move money to finance their terrorist acts are, according to Freeman and Ruehsen (2013), the following:

- **Cash couriers.** They move physical cash from one place to another, the 'simplest and oldest way of moving value' (Passas, 2003). When moving cash across international borders, terrorists typically conceal it in vehicles, packages, luggage or anything else that can hold large physical volumes of cash. When borders are uncontrolled or where the state's resources are strained, they do not even conceal the cash (Money Laundering and Threat Assessment Working Group, 2005).
- **Informal transfer systems.** There are several types of informal and traditional financial networks (Passas, 2003), in particular the widely used *hawala* ⁽¹⁶²⁾. These networks operate in areas where the

⁽¹⁵⁸⁾ European Commission communication COM(2015) 185 final.

⁽¹⁵⁹⁾ In 2008, the FATF's mandate was expanded to include dealing with the financing of proliferation of weapons of mass destruction (Recommendation 7).

⁽¹⁶⁰⁾ Navanti, 'The periodic table of terrorist groups' (<https://www.navantigroup.com/news-1/2018/3/7/navanti-releases-updated-periodic-table-of-terrorist-groups>).

⁽¹⁶¹⁾ World Economic Forum, 'How terrorists fund their attacks — and how to stop them' (<https://www.weforum.org/agenda/2017/11/terror-attacks-are-increasingly-self-funded-how-can-we-stop-them/>).

⁽¹⁶²⁾ *Hawala* networks are 'age-old methods of conducting financial transactions across various borders and cultures using a system of trust and social investment' (Hariharan, 2012). Belonging originally to the Islamic tradition, they operate in the following manner: a

formal banking sector is less established or where large ethnic diasporas live. Although most countries have legalised *hawala*, many *hawaladars* (*hawala* dealers) also operate illegally because of prohibitively high fees (licensing and registration). After 9/11, as a result of evidence that the Taliban and Al-Qaeda in Iraq had used them, they were closely monitored.

- **Money service businesses (MSBs).** MSBs are ‘currency dealers or exchangers; check cashers; issuers (or redeemers) of traveller’s checks, money orders, or stored value cards; and money transmitters’ ⁽¹⁶³⁾. MSBs are subject to the same regulations and laws as banks, including regulatory audits; however, they do not carry out similarly rigorous ‘know your customer’ procedures. Nor does a customer need to have an existing account; a valid form of identification is enough. Most MSBs, and particularly the more established ones, such as Western Union, transfer funds quickly (within minutes to most locations), are inexpensive and offer a low risk of detection, especially if the MSB is unregistered.
- **Formal banking.** This is done by depository financial institutions, such as banks, savings and loan institutions, and credit unions. They are the only entities allowed ‘to engage in the business of receiving deposits and providing access to those deposits’ through a payment system of cheques, electronic networks, credit and debit cards, and bank-to-bank transfers ⁽¹⁶⁴⁾. They are generally heavily regulated and required to maintain records, know their customers, report transactions over a certain threshold and report any suspicious transactions. Despite these safeguards, they continue to be abused by terrorists and other criminals, particularly when a bank asks no questions (e.g. the former al-Madina Bank in Lebanon) (Freeman and Ruehsen, 2013). Alternatively, if a bank is careless, it could be abused by way of correspondent accounts or payable-through accounts of correspondent banks (e.g. in the case of HSBC) (Freeman and Ruehsen, 2013). And, finally, there may be cases where a bank does all it is required to do with respect to customer due diligence, but the transactions still fail to raise any red flags (e.g. the 9/11 hijackers’ accounts).
- **False trade invoicing.** This is one of the most difficult laundering methods to detect, although it is widely used by both organised crime and terrorist groups (Ruehsen, 2001). It disguises the transmission of value from one jurisdiction to another by over- or under-invoicing (Zdanowicz, 2009). For example, if a terrorist based in the United States purchases American honey and then exports it to Yemen, he could overprice the shipment by USD 100 000 without attracting much attention. The additional USD 100 000 goes to the terrorist who arranged for the shipment in the United States. According to one government source, this is believed to have happened in the months leading up to 9/11 (Miller and Gerth, 2001). The detection risk is still relatively low; however, with the establishment of trade transparency units around the world, this risk is rising. In addition to assisting with port security, these units attempt to scour big data, searching for unusually priced transactions ⁽¹⁶⁵⁾.
- **High-value commodities.** Gold and diamonds are two main goods that are smuggled by terrorists across borders. They are both reliable, as they are easily converted into cash, easy to transport and also very difficult to trace (Cassara and Jorisch, 2010). However, it is important to note that obtaining gold and diamonds from the source (such as an African mine) is neither simple nor convenient, as they have to be transported by courier, which comes with a theft risk and at a price.
- **Other methods.** There are three other methods worth mentioning, which could be used more in the future:
 - Stored value cards: they can be ‘closed’ cards that are tied to a particular business, or ‘open’ cards, such as prepaid debit cards, which can be used anywhere. These cards, especially the open ones, ‘provide a compact, easily transportable, and potentially anonymous way’ to move funds (Money Laundering and Threat Assessment Working Group, 2005);

worker in Dubai, for example, wants to send USD 1 000 to his wife in Pakistan. He finds a *hawaladar* and gives him the funds. The *hawaladar* contacts a fellow *hawaladar* in Pakistan. The *hawaladar* in Dubai gives both the worker in Dubai and the *hawaladar* in Pakistan a transaction code. The worker’s wife goes to the *hawaladar* in Pakistan and gives him the code. If the codes match, the *hawaladar* in Pakistan gives the wife the rupee equivalent of USD 1 000 minus a small fee. (Note that no funds have actually crossed borders.) To settle the accounts, the simplest method is for the *hawaladars* to wait for a similar value of transactions to move in the other direction. As this rarely occurs, the *hawaladars* will periodically balance their books by using money service businesses, smuggling high value commodities or making false trade invoicing transactions to transfer funds (see Jost and Sandhu, 2000; Freeman and Ruehsen, 2013).

⁽¹⁶³⁾ United States Bank Secrecy Act definition (Money Laundering and Threat Assessment Working Group, 2005).

⁽¹⁶⁴⁾ United States Bank Secrecy Act definition (Money Laundering and Threat Assessment Working Group, 2005).

⁽¹⁶⁵⁾ US Immigration and Customs Enforcement, ‘ICE leads trade-based money-laundering investigations’ (<https://www.ice.gov/trade-transparency>).

- Casinos: they are known to have been used for criminal money laundering; however, terrorists could potentially use them also to move funds;
- Virtual currencies: these digital currencies (e.g. Bitcoin) are increasingly being used by criminals, especially drug dealers. Although there are only a few confirmed cases, terrorists have started to use virtual currencies to finance terrorism (European Parliament, 2018b).

One of the biggest challenges in combating terrorism financing is the early identification of self-funding lone actors and small cells by financial institutions (European Parliament, 2018b). As movement of money can remain below legislative thresholds, it can be very difficult to distinguish such terrorism financing alert signals from the noise of normal everyday cash movements in society (grocery shopping, online goods shopping, utility payments, etc.).

2.9.3 Countering terrorism financing in the European Union

The European Commission has placed combating terrorism financing at the core of the EU's strategy for fighting against terrorism. It endeavours to ensure that the EU adapts its legal instruments and measures to address the way terrorists and their sponsors constantly evolve their methods of raising, moving and using funds. In 2016, an action plan for strengthening the fight against terrorism financing was launched ⁽¹⁶⁶⁾. It focuses on two main strands:

- tracing terrorists through financial movements and preventing them from moving funds or other assets, to ensure that financial movements can wherever possible help law enforcement to trace terrorists and stop them from committing crimes;
- disrupting the sources of revenue used by terrorist organisations, by targeting their capacity to raise funds.

In this action plan, the main activities geared to preventing movement of funds and identifying terrorist funding are:

- ensuring virtual currency exchange platforms are covered by the anti-money laundering directive;
- tackling terrorism financing through anonymous pre-paid instruments;
- improving access to information for and cooperation between EU financial intelligence units;
- ensuring a high level of safeguards for financial flows from high-risk non-EU countries;
- giving EU financial intelligence units access to centralised bank and payment account registers and central data retrieval systems.

The action plan also mentions the main activities focused on disrupting revenue sources for terrorist organisations:

- tackling terrorism financing sources such as illicit trade in cultural goods and wildlife;
- working with non-EU countries to ensure a global response to tackling terrorism financing sources.

In particular, the EU has developed measures to cut off terrorists' access to funding. In 2005, the third anti-money laundering directive ⁽¹⁶⁷⁾ expressly widened the scope of the anti-money laundering regime to terrorism financing; it was followed by the fourth anti-money laundering directive ⁽¹⁶⁸⁾. In July 2018, the fifth anti-money laundering directive ⁽¹⁶⁹⁾ was issued, aiming to:

- increase transparency about who owns companies and trusts to prevent money laundering and terrorism financing using opaque structures;
- improve the work of financial intelligence units, with better access to information through centralised bank account registers;

⁽¹⁶⁶⁾ European Commission, Commission communication, 'Action plan for strengthening the fight against terrorist financing', (COM(2016) 50 final), Strasbourg, 2.2.2016.

⁽¹⁶⁷⁾ Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing, OJ L 309, 25.11.2005, p. 15-36.

⁽¹⁶⁸⁾ Directive (EU) 2015/849.

⁽¹⁶⁹⁾ Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU, OJ L 156, 19.6.2018, p. 43-74.

- tackle terrorism financing risks linked to anonymous use of virtual currencies and pre-paid instruments;
- improve the cooperation and exchange of information among anti-money laundering supervisors and between supervisors and the European Central Bank;
- broaden the criteria for assessing high-risk non-EU countries and ensure a common high level of safeguards for financial flows from such countries.

In October 2005, the regulation on cash control⁽¹⁷⁰⁾ was launched, requiring that cash in excess of EUR 10 000 be disclosed to competent authorities when entering or leaving the EU. This regulation aimed to introduce preventive action to fight money laundering and terrorism financing with the help of more effective customs cooperation.

In November 2006, two other legal acts were adopted in the EU.

- The regulation on funds transfers implements FATF Recommendation 7, ensuring that wire transfers are accompanied by identifying information. In particular, it lays down rules to ensure the traceability of transfers of funds. These rules are applicable to all payment service providers involved in the payment chain⁽¹⁷¹⁾.
- The payments services directive addresses FATF Recommendation 6 on alternative remittances. In particular, it lays down rules on payment services, such as credit transfers, direct debits and card payments. These rules include information requirements for payment services providers, including rights and obligations linked to the use of payment services⁽¹⁷²⁾.

In addition, there are Council common positions on combating terrorism regarding procedures for listing persons and entities related to terrorism, from 2001 and 2009⁽¹⁷³⁾. Their objective is to establish a list of individuals, groups and entities involved in terrorism whose funds and other financial assets are to be frozen as part of the fight against the financing of terrorism.

The European Commission is an active member of the FATF, contributing in particular to the implementation of its recommendations. The Commission also cooperates with the UN and ensures that all relevant UN resolutions⁽¹⁷⁴⁾ and Council of Europe instruments, such as the Council of Europe Convention No. 198⁽¹⁷⁵⁾, play an important role in this context.

There is also a very good practical collaboration between the EU (the European Commission and Europol) and the United States (the CIA and the US Treasury Department) under the TFTP set up by the US Treasury Department in the aftermath of the 9/11 attacks. Soon thereafter, the EU–US TFTP Agreement was sealed; it brought together US-led intelligence analytics and checks and balances modelled on European values (de Goede and Wesseling, 2017). Since 2012, the EU has had its own overseer inside the US Treasury to formally control the treaty agreements. More than 1 500 intelligence leads have been shared across the Atlantic thanks to this cooperation (de Goede and Wesseling, 2017).

Finally, some studies commissioned by the European Commission revealed that NGOs are potentially vulnerable to exploitation for terrorism financing (Matrix Insight, 2008; European Parliament, 2015b). The Commission aims to work closely with the NGO sector and EU Member States in this area.

⁽¹⁷⁰⁾ Regulation (EC) No 1889/2005 of the European Parliament and of the Council of 26 October 2005 on controls of cash entering or leaving the Community, OJ L 309, 25.11.2005, p. 9–12.

⁽¹⁷¹⁾ Regulation (EC) No 1781/2006 of the European Parliament and of the Council of 15 November 2006 on information on the payer accompanying transfers of funds, OJ L 345, 8.12.2006, p. 1–9.

⁽¹⁷²⁾ Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC, OJ L 337, 23.12.2015, p. 35–127.

⁽¹⁷³⁾ Council of the European Union, Council common position on combating terrorism (2001/930/CFSP), Brussels, 27.12.2001; Council of the European Union, Council common position updating common position 2001/931/CFSP on the application of specific measures to combat terrorism and repealing common position 2009/67/CFSP (2009/468/CFSP), Luxembourg, 15.6.2009.

⁽¹⁷⁴⁾ <http://www.un.org/en/documents/>; consulted on 6 August 2018.

⁽¹⁷⁵⁾ <http://conventions.coe.int/Treaty/EN/Treaties/html/198.htm>; consulted on 6 August 2018.

2.9.4 Possible evolution of terrorism financing within the next 5 years

According to Neumann⁽¹⁷⁶⁾, efforts to combat terrorism financing have mainly focused on banks and financial institutions. He highlights four important issues that should be taken into account when following the money:

- **Cash.** It has been observed that most ISIS transactions have been in cash, because most people (98 %) in Syria and Iraq do not possess bank accounts and fewer have credit cards. Therefore, seeking ISIS's money in the international financial system is unlikely to be successful. When dealing with ISIS, following the money means following the cash.
- **Territory.** When terrorist organisations hold territory, they start working within it by taxing people and selling resources, such as oil. This makes it very difficult to cut them off from outside. Therefore, cutting off their finances means taking away their territory by defeating them on the ground.
- **Smuggling.** Terrorists in conflict zones tend to be closely linked to illegal economies where smugglers have been working long before ISIS, Al-Qaeda or the Taliban existed. Thus, countering terrorism finance means countering illicit economies.
- **Small-dollar terrorism.** Since 2014, none of the attacks in Europe have cost more than EUR 10 000. In fact, the majority cost less than EUR 1 000. Often, they were funded by the terrorists themselves, who used their savings, salaries or money they had borrowed from friends or parents. Others were funded from the proceeds of crime. In practice, none went through the formal financial system, resulting in no suspicious transactions that could have been identified.

Against this backdrop, the same author recommends the following:

- **Evidence-based countering of terrorism finance.** Responses to terrorism financing must fit the reality. That can mean doing different things in different places. In some cases, it may involve the international financial system.
- **Holistic approach to countering terrorism finance.** Too much focus has been on the financial sector. There is a need to complement financial tools with political, diplomatic, military and law enforcement tools. In many cases, this requires partnerships with the private sector.
- **Integrated approach to countering terrorism finance.** There is a need to be more integrated with the rest of counterterrorism. Countering terrorism finance has been practised as an activity that is completely separate from the rest of counterterrorism.

Complementing the abovementioned list of challenges, the FATF (2015a) provides its own list:

- **Understanding the nature of an isolated transaction (e.g. a money transfer).** Is it legitimate (e.g. a family remittance) or nefarious (e.g. used to support a terrorist group)? Financial intelligence units and operational authorities need to improve their ability to cooperate with the intelligence community and specific interagency task forces may need to be established.
- **Rapid expansion of social media.** This is a relatively new worldwide channel of exploitation used by terrorist groups to raise funds. Through targeted propaganda, social networks are used to coordinate large-scale and well-organised fundraising schemes (crowdfunding, fundraising through pre-paid cards and e-wallets) aimed at terrorism financing, which may involve several thousand sponsors and may raise significant amounts of cash.
- **Exploitation of natural resources.** Such activities allow terrorist organisations to control and occupy territory by sustaining burgeoning criminal activity related to this sector, such as extortion, smuggling, theft, illegal mining, kidnapping for ransom, corruption and other environmental crimes. The natural resources commonly exploited by terrorist groups are oil and gas, and mining.

⁽¹⁷⁶⁾ See International Centre for the Study of Radicalisation, 'Beyond banking: Professor Neumann's opening keynote address at 'No money for terror' summit in Paris' (<https://icsr.info/2018/04/26/beyond-banking-professor-neumanns-opening-keynote-address-no-money-terror-summit-paris/>).

Terrorist groups are increasingly relying on closed chat programs, as social networks have become heavily monitored by law enforcement institutions. Monitoring of these private communications is virtually impossible. An American strategy to install a backdoor in software by coercion has proven disastrous ⁽¹⁷⁷⁾.

Cryptocurrencies have not been used frequently by terrorist groups, so their contribution to financing terrorism is so far negligible; nonetheless, a regulation is needed. It should be taken into consideration that, like money transfer operators and informal money transfer channels, digital currencies have begun to be used by migrants to send money home. Any anti-terrorism regulation should take this into consideration ⁽¹⁷⁸⁾.

2.9.5 Stakeholders

2.9.5.1 European Union stakeholders

European Commission Directorate-General for Migration and Home Affairs

DG Migration and Home Affairs manages policies that aim to ensure that all activities necessary and beneficial to the economic, cultural and social growth of the EU can develop in a stable, lawful and secure environment. In particular, it looks at how terrorism financing links with organised crime, feeding terrorism through channels such as the supply of weapons, proceeds from drug smuggling and the infiltration of financial markets.

In the effort to combat terrorism financing, the European Commission's role is to support Member States. Through the DG's Directorate E, Migration and Security Funds — Financial Resources and Monitoring, funding is provided to projects addressing this topic.

https://ec.europa.eu/home-affairs/what-we-do/policies/crisis-and-terrorism/financing_en

European External Action Service

The EEAS is the EU's diplomatic service. A key aspect of the work of the EEAS is its ability to work closely with the foreign and defence ministries of the EU Member States and with EU institutions. It also has a strong working relationship with the UN and other international organisations. It helps the HR/VP to implement the EU's CFSP.

In 2016, the EU took unprecedented steps to increase internal cooperation in the field of security and defence. The HR/VP launched the EU global strategy on security and defence, which aims to invest in a stronger EU and, at the same time, in a stronger cooperation with EU partners. Combating terrorism financing is one of the priorities of the global strategy.

https://eeas.europa.eu/headquarters/headquarters-homepage_en

European Union Agency for Law Enforcement Cooperation (Europol)

Europol is the EU's law enforcement agency. It supports the EU Member States in their fight against terrorism, cybercrime and other serious and organised forms of crime. It also works with many non-EU partner states and international organisations.

In January 2016, Europol created the ECTC, which is an operations centre and hub of expertise that aims to strengthen the EU's response to terror and ensure an effective response to terrorism-related challenges. The ECTC focuses on several activities, including sharing intelligence and expertise on terrorism financing (through the TFTP and financial intelligence units). It also carries out the following activities:

- provision of operational support for investigations upon request from an EU Member State;
- tackling foreign fighters;
- addressing online terrorist propaganda and extremism (through the EU IRU);
- fighting against illegal arms trafficking;
- international cooperation among counterterrorism authorities.

⁽¹⁷⁷⁾ Counter Extremism Project, 'Terrorists on Telegram' (<https://www.counterextremism.com/terrorists-on-telegram>); Vox, 'Terrorists' love for Telegram, explained' (<https://www.vox.com/world/2017/6/30/15886506/terrorism-isis-telegram-social-media-russia-pavel-durov-twitter>).

⁽¹⁷⁸⁾ <https://cointelegraph.com/news/crypto-is-a-poor-form-of-money-for-terrorists-congressional-hearing-concludes>; consulted on 4 December 2018.

Since 2007, Europol has made available to the public EU terrorism situation and trend reports (Europol, 2017, 2018b). These provide the European Parliament and all national governments and police forces with an annual overview of the European terrorism situation. A section of each report is dedicated to terrorism financing.

<https://www.europol.europa.eu/about-europol/european-counter-terrorism-centre-ectc>

Eurojust

Eurojust was established in 2002 as the EU's Judicial Cooperation Unit. It is considered central to the EU's pursuit pillar, for its capacity to improve cooperation between judicial authorities in tackling terrorism financing and depriving terrorists of their means of attack and communication. Eurojust has consistently aided in the investigation and prosecution of cross-border terrorism cases by coordinating cooperation among Member States and building relationships with judicial authorities in non-EU countries.

<http://www.eurojust.europa.eu/Pages/home.aspx>

2.9.5.2 International stakeholders

United Nations Office on Drugs and Crime, Terrorism Prevention Branch

The Terrorism Prevention Branch of UNODC works on the legal aspects of countering the financing of terrorism, including promoting the ratification of the relevant universal legal instruments, in particular the International Convention for the Suppression of the Financing of Terrorism (Tofangsaz, 2018), and the implementation of these international standards. This entails reviews of domestic legislation, to ensure proper criminalisation of offences related to the financing of terrorism, and legislative drafting, developing the capacity of criminal justice and law enforcement officials to investigate, prosecute and adjudicate terrorism financing through the provision of specialised training on issues related to special investigation techniques, freezing, seizing and confiscating terrorist assets, and strengthening regional and international cooperation against the financing of terrorism.

<https://www.unodc.org/unodc/en/terrorism/news-and-events/terrorist-financing.html>

Financial Action Task Force

The FATF is an intergovernmental body established in 1989 to build on the G7's efforts to develop policies to combat money laundering in drug trafficking. In 2001, it widened its mandate to include terrorism financing. Its objectives are to set standards and promote the effective implementation of legal, regulatory and operational measures to combat money laundering, terrorism financing and other related threats to the integrity of the international financial system. The FATF is therefore a policymaking body that works to generate the necessary political will to bring about national legislative and regulatory reforms in these areas. In particular, it monitors progress in implementing the 40 FATF Recommendations⁽¹⁷⁹⁾. It works in collaboration with other international stakeholders to identify national-level vulnerabilities with the aim of protecting the international financial system from misuse. The FATF Secretariat is housed at the OECD headquarters in Paris.

<http://www.fatf-gafi.org/>

Global Initiative against Transnational Organized Crime

The Global Initiative was founded in 2013 and headquartered in Geneva. It comprises a network of nearly 300 independent global and regional experts working on human rights, democracy, governance and development issues, in relation to which organised crime has become increasingly pertinent.

It provides a platform to promote greater debate and innovative approaches as the building blocks for an inclusive global strategy against organised crime. It commissions and shares research globally, curates a robust resource library of 2 000 reports and tools specific to organised crime, and uses its tremendous convening power to unite the private and public sectors against organised crime.

The Global Initiative seeks to project the expertise of its members outwards and to make it available to a broad range of stakeholders, including by developing the evidence basis for policymaking, convening and

⁽¹⁷⁹⁾ The FATF developed 40 recommendations that are recognised as the international standard for countering money laundering and financing of terrorism and proliferation of weapons of mass destruction. They were first issued in 1990 and were revised in 1996, 2001, 2003 and 2012 to ensure that they remain relevant.

facilitating multisectoral dialogue, and developing tools and programmes needed to further the development of effective responses.

<http://globalinitiative.net>

North Atlantic Treaty Organization

NATO is a political-military alliance between 29 member states who have agreed to mutual defence based on the North Atlantic Treaty, signed on 4 April 1949, in response to an attack by any external party. NATO's headquarters are located in Brussels, Belgium, while the headquarters of Allied Command Operations is near Mons, Belgium. NATO's purpose is to guarantee the freedom and security of its members through the following means:

- political — by promoting democratic values and promoting members to consult and cooperate on defence- and security-related issues to solve problems, build trust and, in the long run, prevent conflict;
- military — if diplomatic efforts fail, NATO has the military power to undertake crisis management operations, which are executed under the collective defence clause of NATO's founding treaty, under Article 5 of the Washington Treaty or under a UN mandate, alone or in cooperation with other countries and international organisations.

As part of its counterterrorism strategy, NATO collects intelligence in a multidisciplinary manner through cooperation across sectors and among member states on many fronts: defence, diplomacy, healthcare, law enforcement, the military and finance. In 2005, NATO, together with UNODC and OSCE, agreed on the need to gather and exchange data on terrorism financing and develop relevant international financial standards ⁽¹⁸⁰⁾.

<https://www.nato.int/>

International Monetary Fund (IMF)

The IMF is an organisation of 189 countries that works to foster global monetary cooperation, secure financial stability, facilitate international trade, promote high employment and sustainable economic growth, and reduce poverty around the world. Created in 1945, the IMF is governed by and accountable to its member countries. Like money laundering, terrorism financing can threaten a country's economic stability. Thus, IMF is very active in supporting and promoting the FATF recommendations among IMF member countries. After 20 years, combating terrorism financing has become part of IMF's core work, with activities including analysis and policy advice, assessing the health and integrity of financial sectors, providing financial assistance when needed, and helping countries build institutions and increase operational effectiveness.

<http://www.imf.org/external/np/leg/amlcft/eng/>

International Criminal Police Organisation (Interpol)

Interpol's Counter-Terrorism Fusion Centre investigates the organisational hierarchies, training, financing, methods and motives of terrorist groups. Its activities are global in scope and implemented through regionally focused but interlinked projects. The aim is to improve the exchange of law enforcement information across borders and to enrich law enforcement practices. Interpol considers disrupting money flows of terrorist groups to be a fundamental pillar of its worldwide efforts to combat terrorism. It currently has information on over 43 000 foreign terrorist fighter profiles, which the world's police can access and consult. Its Criminal Analysis File (300 000 entities) includes financial identifiers and phone numbers. This growing repository of multidisciplinary and multisectoral intelligence information facilitates the mapping and understanding of critical information chain linkages among terrorist activities.

<https://www.interpol.int/Crimes/Terrorism>

2.9.6 Legislation and reference documents

- Council Regulation (EC) No 2580/2001 of 27 December 2001 on specific restrictive measures directed against certain persons and entities with a view to combating terrorism, OJ L 344, 28.12.2001, p. 70-75.
- Council Framework Decision 2002/475/JHA of 13 June 2002 on combating terrorism, OJ L 164, 22.6.2002, p. 3-7.

⁽¹⁸⁰⁾ NATO, 'International organisations join forces to combat terrorist financing' (https://www.nato.int/cps/su/natohq/news_21590.htm?selectedLocale=en).

- European Commission, Commission communication, 'Prevention of and the fight against terrorist financing through measures to improve the exchange of information, to strengthen transparency and enhance the traceability of financial transactions' (COM(2004) 700 final), Brussels, 20 October 2004.
- European Commission, Commission communication, 'Preparedness and consequence management in the fight against terrorism' (COM(2004) 701 final), Brussels, 20 October 2004.
- Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing, OJ L 309, 25.11.2005, p. 15-36.
- European Commission, Commission communication, 'The prevention of and fight against terrorist financing through enhanced national level coordination and greater transparency of the non-profit sector' (COM(2005) 620 final), Brussels, 29 November 2005.
- Regulation (EC) No 1781/2006 of the European Parliament and of the Council of 15 November 2006 on information on the payer accompanying transfers of funds, OJ L 345, 8.12.2006, p. 1-9.
- Council Decision 2007/124/EC, Euratom, of 12 February 2007 establishing for the period 2007 to 2013, as part of General Programme on Security and Safeguarding Liberties, the Specific Programme 'Prevention, Preparedness and Consequence Management of Terrorism and other Security-related risks', OJ L 58, 24.2.2007, p. 1-6.
- European Commission, Commission communication, 'Stepping up the fight against terrorism' (COM(2007) 649 final), Brussels, 6 November 2007.
- Directive 2007/64/EC of the European Parliament and of the Council of 13 November 2007 on payment services in the internal market amending Directives 97/7/EC, 2002/65/EC, 2005/60/EC and 2006/48/EC and repealing Directive 97/5/EC, OJ L 319, 5.12.2007, p. 1-36.
- Council Decision 2010/412/EU of 13 July 2010 on the conclusion of the agreement between the European Union and the United States of America on the processing and transfer of financial messaging data from the European Union to the United States for the purposes of the Terrorist Finance Tracking Program, OJ L 195, 27.7.2010, p. 3-4.
- European Commission, Commission communication, 'The EU counter-terrorism policy: main achievements and future challenges' (COM(2010) 386 final), Brussels, 20 July 2010.
- European Commission, Commission communication, 'A European terrorist finance tracking system: available options' (COM(2011) 429 final), Brussels, 13 July 2011.
- European Commission. Commission staff working document, 'Report on the second joint review of the implementation of the agreement between the European Union and the United States of America on the processing and transfer of financial messaging data from the European Union to the United States for the purposes of the Terrorist Finance Tracking Program' (SWD(2012) 454 final), Brussels, 14 December 2012.
- European Commission, Commission communication, 'A European terrorist finance tracking system (EU TFTS)' (COM(2013) 842 final), Brussels, 27 November 2013.
- European Commission, Commission communication, 'Pursuant to Article 294(6) of the Treaty on the Functioning of the European Union concerning the position of the Council on the adoption of a directive of the European Parliament and of the Council on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing' (COM(2015) 188 final), Brussels, 27 April 2015.
- European Commission, Commission communication, 'The European agenda on security' (COM(2015) 185 final), Strasbourg, 28 April 2015.
- Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC, OJ L 141, 5.6.2015, p. 73-117.

- Regulation (EU) 2015/847 of the European Parliament and of the Council of 20 May 2015 on information accompanying transfers of funds and repealing Regulation (EC) No 1781/2006, OJ L 141, 5.6.2015, p. 1-8.
- European Commission, Commission communication, 'Action Plan for strengthening the fight against terrorist financing' (COM(2016) 50 final), Strasbourg, 2 February 2016.
- European Commission, Commission communication, 'Delivering on the European agenda on security to fight against terrorism and pave the way towards an effective and genuine security union' (COM(2016) 230 final), Brussels, 20 April 2016.
- European Commission, Commission report, *On the joint review of the implementation of the agreement between the European Union and the United States of America on the processing and transfer of financial messaging data from the European Union to the United States for the purposes of the Terrorist Finance Tracking Program* (COM(2017) 31 final), Brussels, 19 January 2017.
- Directive (EU) 2017/541 of the European Parliament and of the Council of 15 March 2017 on combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA, OJ L 88, 31.3.2017, p. 6-21.
- European Commission, 'Reflection paper on the future of European defence' (COM(2017) 315 final), Brussels, 7 June 2017.
- Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU, OJ L 156, 19.6.2018, p. 43-74.

2.10 Space

2.10.1 The importance of space for the European Union and for security

There are two main reasons why space and security come together ⁽¹⁸¹⁾.

First, space is the unique enabler of a number of security and defence applications. These include monitoring areas anywhere on earth and providing unassailable platforms for global positioning and communication for use with security and defence forces. After the launch of Sputnik 1 in 1957, the military forces of the superpowers were the first users of space, followed soon by space exploration missions for scientific and national motivation purposes (the race to the Moon). Classical security and defence uses of space include monitoring of foreign territories for signs of preparation of hostile activities, detection of intercontinental ballistic missile launches for immediate response, global positioning and navigation to support global military operations, and global communications links for command and control. Several of these uses have contributed to global stability in the past 60 years. The essential advantages of using space-based platforms for this are global reach and unassailability.

The second main link between space and security is that today the economy and society have become dependent on space, primarily again because of space-based navigation and communication services, and also because of weather services. Any disruption would have grave economic consequences, and therefore the health of space assets has become a matter of security. We rely on communication satellites for broadcasting (television) and to communicate with ships, aeroplanes and remote locations, and even more strongly on positioning signals for the navigation of aeroplanes, ships, cars and individuals. Furthermore, weather services depend on satellite monitoring of the atmosphere, and satellite imaging of the Earth's surface (Earth observation) enables a range of applications from making maps to agriculture control and global climate change monitoring. Space-based commercial applications are being expanded and contribute to significant economic (service provider) activity.

While the abovementioned interests — the security and economic applications of space — are in the first instance national, investments in space can be huge. Historically, it was the superpowers, the United States

⁽¹⁸¹⁾ In 2018, a thorough landscape study dedicated to space and security was performed by the JRC with the help of an external contractor (Lagazio et al., 2019). It involved a survey of policies, stakeholders, capabilities and R & D at EU level and in eight individual European countries selected on the basis of their total national space budget (France, Germany, Italy, the United Kingdom, Spain, Belgium, Sweden and Norway). It also indicated policy and capability gaps, and made recommendations for R & D. Much of the content of this chapter is based on that study.

and the Soviet Union, that were the first to benefit from space. Later, some large European countries followed (the United Kingdom, France), but their separate budgets of course could not match those of the superpowers. European countries have therefore pooled their resources, first through the European Space Agency (ESA) and later (in addition) at EU level.

It is helpful to categorise space matters as follows:

- space exploration and science — missions to the Moon and the planets, human space flight, astronomical satellites, space-based research and manufacturing;
- communication and broadcasting — satellite TV and phones, military communications satellites, mainly from geostationary satellites, many commercially operated;
- observation — meteorology, Earth observation, spy satellites;
- positioning, navigation and timing (PNT) — includes the United States' Global Positioning System (GPS), Galileo (Europe's GNSS) and the European Geostationary Navigation Overlay Service (EGNOS), and similar GNSS and regional ones from Russia, China and Japan;
- space situational awareness (SSA) with three components — space surveillance and tracking (SST) to monitor satellites and debris in orbit and prevent collisions, monitoring of space weather to be warned of solar storms and their impact on earth, and monitoring of near-Earth objects (NEO) to be warned of impending impacts of asteroids and the like;
- enabling structures — includes hard infrastructures such as launchers, launch facilities and ground stations, but also manufacturing (of launchers, vehicles, payloads) and service provision, and also aspects such as supply chain, general (critical) infrastructure (power supply, land communications, etc.), education, capacity building and governance.

2.10.2 The European Union's role and ambition in space

The first European pooling of space activities was done by setting up the ESA in 1975. To this day, the ESA, as an intergovernmental organisation of 22 member states, has a leading role in European space efforts. Its member states channel part of their national space budget through the ESA in order to be part of a larger European effort. The ESA member states are not exactly the same as the EU Member States. Not all EU Member States participate in the ESA and, conversely, Norway is an ESA member state, as is Canada, although the latter does not have full membership. In spite of this, the EU channels a significant part of its space budget through the ESA for implementation. Particular areas where the ESA is active but the EU is not or is less so are space exploration; scientific (astronomical) satellites; space science, engineering and technology; and operating space assets. The ESA's mandate is limited to peaceful use, but it does consider safety aspects, which sometimes overlap with security. In 2016, the ESA issued 'Towards Space 4.0 for a United Space in Europe' ⁽¹⁸²⁾. The resolution restates the objectives of a United Space in Europe, establishes the ESA's long-term plan and industrial policy, and calls for an optimised ESA for Space 4.0 (a concept that is intended to reflect new aspects of space; see Section 2.10.4).

The EU's mandate for space was set by the 2007 Lisbon Treaty. Specifically, the TFEU says, in Title XIX, 'Research and technological development and space', Article 189, that the Union shall draw up a European space policy, that it shall establish appropriate relations with the ESA, and that the European Parliament and the Council may establish a European space programme.

Already before that, in 2003, the Commission published a White Paper entitled 'Space: a new European frontier for an expanding Union — an action plan for implementing the European space policy' ⁽¹⁸³⁾. Then, in 2007, the Commission published the European space policy ⁽¹⁸⁴⁾. It aims to foster better coordination of space activities between the EU, the ESA and their respective Member States, to maximise value for money and avoid unsustainable duplication, thus meeting shared European needs. Increased synergies between civil and defence space programmes and technologies are also targeted. It emphasises the importance of meeting Europe's security and defence needs as regards space, and supporting Earth observation for security and defence and autonomous access to information relating to the environment, climate change and security,

⁽¹⁸²⁾ ESA, 'Ministerial Council 2016' (https://www.esa.int/About_Us/Ministerial_Council_2016).

⁽¹⁸³⁾ European Commission, 'White Paper: space — a new European frontier for an expanding Union: an action plan for implementing the European Space policy' (COM(2003) 673 final), Brussels, 11.11.2003.

⁽¹⁸⁴⁾ European Commission, Commission communication, 'European space policy' (COM(2007) 212 final), Brussels, 26.4.2007.

which is of strategic importance for Europe. It underlines that space assets make a significant contribution to security and defence.

The of the Council of the European Union resolutions of 2010 'Taking forward the European space policy of 2008' ⁽¹⁸⁵⁾ and 'Global challenges: taking full benefit of European space systems' (Council of the European Union and Council of the European Space Agency, 2010) encouraged space developments, underlining European autonomy, innovation, EU-ESA coordination and the relation to security.

In 2010, the GSA was set up ⁽¹⁸⁶⁾, and in 2014 the EU established the Copernicus programme ⁽¹⁸⁷⁾. Copernicus is a civil, user-driven programme which builds on the previous European Earth observation programme, Global Monitoring for Environment and Security, as well as on existing related national and European capacities. The objective of Copernicus is to provide accurate and reliable information in the field of the environment and security, tailored to the needs of users and supporting other EU policies, in particular relating to the internal market, transport, the environment, energy, civil protection and civil security, cooperation with non-EU countries and humanitarian aid.

In 2016, the European Commission published its space strategy for Europe ⁽¹⁸⁸⁾, which focuses on:

- maximising the benefits of space for society and the EU economy;
- fostering a globally competitive and innovative European space sector;
- reinforcing Europe's autonomy in accessing and using space in a secure and safe environment;
- strengthening Europe's role as a global actor and promoting international cooperation;
- promoting partnerships between the actors — the Commission, the EU Member States, the ESA, the GSA, the European Organisation for the Exploitation of Meteorological Satellites (EUMETSAT), the EEAS, relevant agencies, industry, and research and user communities.

Propelled by all this political will, the EU has indeed taken on a major role in space. It has developed two flagship programmes in space, Galileo/EGNOS for PNT and Copernicus for Earth observation. EGNOS provides augmentation services in Europe for positioning and navigation, augmenting the existing GPS, and thus enabling a number of specialist and safety-critical applications. Galileo encompasses a satellite constellation that provides global PNT services independently of GPS, and with greater accuracy and reliability. Copernicus consists of six constellations of EU-owned satellites with different Earth observation capacities (optical, radar, sea, atmosphere, etc.) plus six services aimed at broad application domains that use, in addition to the data from the Copernicus satellites, data from other satellites and non-space sources. With these capabilities, the EU makes a contribution at the level of other big players such as the United States.

The EU's investments in space are not only done to provide it with autonomous capabilities in PNT and Earth observation. The EGNOS, Galileo and Copernicus core services and data are provided for free, with the aim of stimulating (European) business. The EU deploys targeted activities to stimulate the development of businesses, including SMEs, in the space sector and downstream service sector.

In addition to these two flagship programmes, the EU carries out activities on coordinating SST among the EU Member States and on stimulating research and innovation related to space. Attention is also paid to launch capabilities. A framework for SST support ⁽¹⁸⁹⁾ was established in 2014; it aims to help protect satellites from space debris. Research is mainly dealt with through the European research framework programmes (see Section 3.1).

Specifically on the security aspect of space, from the European Parliament there have been two resolutions, one in 2008 on space and security ⁽¹⁹⁰⁾ and another in 2016 on space capabilities for European security and defence ⁽¹⁹¹⁾. Together, they call for the geospatial intelligence necessary for autonomous EU threat

⁽¹⁸⁵⁾ Council Resolution of 26 September 2008, 'Taking forward the European Space Policy', OJ C 268, 23.10.2008, p. 1-6.

⁽¹⁸⁶⁾ Regulation (EU) No 912/2010 of the European Parliament and of the Council of 22 September 2010 setting up the European GNSS Agency, repealing Council Regulation (EC) No 1321/2004 on the establishment of structures for the management of the European satellite radio navigation programmes and amending Regulation (EC) No 683/2008, OJ L 276, 20.10.2010, p. 11-21.

⁽¹⁸⁷⁾ Regulation (EU) No 377/2014 of the European Parliament and of the Council of 3 April 2014 establishing the Copernicus Programme and repealing Regulation (EU) No 911/2010, OJ L 122, 24.4.2014, p. 44-66.

⁽¹⁸⁸⁾ European Commission, Commission communication, 'Space strategy for Europe' (COM(2016) 705 final), Brussels, 26.10.2016.

⁽¹⁸⁹⁾ Decision No 541/2014/EU of the European Parliament and of the Council of 16 April 2014 establishing a framework for space surveillance and tracking support, OJ L 158, 27.5.2014, p. 227-234.

⁽¹⁹⁰⁾ European Parliament Resolution 2008/2030(INI) on space and security, Strasbourg, 10 July 2008.

⁽¹⁹¹⁾ European Parliament Resolution 2015/2276(INI) on space capabilities for European security and defence, Strasbourg, 8 June 2016.

assessment; the development of precision PNT, Earth observation and reconnaissance; the further development of Galileo and Copernicus for security and defence; secured and interoperable satellite telecommunication systems; SSA, space surveillance and intelligence; the use of space capabilities against ballistic missiles; the protection of space infrastructures (against jamming, spoofing, cyberattacks, space weather and debris); European non-dependence as regards critical space technologies and access to space; international cooperation on space policy, security and missile defence; and policies and research capabilities to open up future applications.

The Council of the European Union issued a decision in 2014 on SatCen⁽¹⁹²⁾, repealing the original establishing joint action of 2001 while reaffirming the continuity of SatCen's operations in the context of the EU's CFSP and, in particular, the CSDP.

The 2016 space strategy for Europe, referred to above, mentions reinforcing synergies between civil and security space activities, and close cooperation of the Commission with the EEAS, the EDA and SatCen, together with Member States and the ESA, to explore possible dual-use synergies arising from the space programmes.

With regard to the security services currently provided by the EU space programmes, Galileo provides some PNT services of extra-high quality that are restricted to authorised governmental users, the Public Regulated Service. One of the six Copernicus services is the Security Service. This is the only part of Copernicus that is not free and open, but only for authorised government users. It currently has three sub-areas, maritime surveillance, border surveillance and support to external action, which is basically outside-EU surveillance. Like the other Copernicus services, it is based on user requirements; in this case, the users are security users for applications such as border control, policing, international treaty control, consular support, conflict monitoring, etc., who work in the EEAS, in EU agencies such as Frontex and the European Fisheries Control Agency, in Member State ministries of defence, in the Commission, etc. Unlike all the other Copernicus services, the products are mostly not based on the Copernicus satellites but on third-party satellites, since the former are designed for global monitoring as opposed to intelligence gathering.

On the defence side, there are currently more bilateral programmes between individual Member States than joint EU level activities in space. SatCen, one of the three EU agencies under the HR/VP, constitutes a joint capability for satellite image intelligence for the Member State ministries of defence. This is military driven, as opposed to Copernicus, which is civil driven. The EDA, also under the HR/VP, has some programmes for assessing joint exploitation of space assets for defence purposes.

2.10.3 The international scene

Space is a 'global commons', a resource shared by all. The sustainability of its use can only be ensured by globally shared responsibility and governance. Therefore, the UN has taken a role from the earliest days in brokering international agreements on the use of space.

The UN also has, of course, a primary role in international security.

Besides its activities on security per se, the UN has several programmes and offices for using space in response to disasters: the UN Platform for Space-based Information for Disaster Management and Emergency Response, the UN Operational Satellite Applications Programme and the UN Office for Disaster Risk Reduction. The UN also oversees the World Meteorological Organization (WMO), which provides the framework for cooperation at a global scale between national meteorological and hydrological services for the development of meteorology, climatology and operational hydrology. WMO runs a space programme with the objective of promoting the availability and use of satellite data and products for weather, climate, water and related applications to WMO member states.

There are five UN treaties on space. In addition, five principles and a number of other resolutions on space have been adopted by the UN General Assembly, the first in 1963. All five treaties are from the 1960s and 1970s. The 1980s and 1990s have seen four resolutions, which deal with contemporary developments such as TV broadcasting and Earth observation.

Since the start of the 2000s, and especially in recent years, there has been less willingness from some key countries to come to new global agreements. This is in spite of urgent need, in view of the ever increasing use of space (the rise in the number of satellites and data links and the amount of space debris). The EU has proposed an international code of conduct for outer-space activities as a contribution to transparency and

⁽¹⁹²⁾ Council Decision 2014/401/CFSP.

confidence-building measures in relation to outer-space activities⁽¹⁹³⁾. However, so far this has not been adopted by the international community and the UN.

While the UN General Assembly is the highest body to adopt positions, in relation to space such positions are typically prepared by the UN Committee on the Peaceful Uses of Outer Space, which comes together in regular sessions with delegates from each member state. It is supported by the UN Office for Outer Space Affairs, which consists of UN staff and which also deploys additional space-related initiatives. One such activity is the Space 2030 agenda⁽¹⁹⁴⁾, which contains recommendations on the contribution of space activities to the achievement of the Sustainable Development Goals, on the wider inclusion of nations and stakeholders in space activities, on increased resilience and sustainability, and on strengthened international governance of space.

It is the EEAS that represents the EU at the UN, including on space and security. However, DG Internal Market, Industry, Entrepreneurship and SMEs also has a remit to deal with the UN on certain space matters.

2.10.4 Possible evolution of space within the next 5 to 10 years

Contemporary developments in technology and the economy are leading to rapid changes in the use of space. This is sometimes referred to as 'New Space' or 'Space 4.0'. It is characterised by the following shifts:

- from involvement in space by a few rich countries to involvement by many countries, including developing ones;
- from a leading role for national space agencies and governmental funding to a leading role for private companies and private funding;
- from a few big, expensive satellites to large constellations of small, cheap satellites;
- from space assets being unassailable and impervious to interference to their being vulnerable to attacks and accidents;
- from space being a limitless resource to space being congested and contested (and the same applies to the radiofrequency spectrum);
- from use of space by specialist communities (science, defence) to the integration of space into the economy and pervasive use.

These shifts bring great opportunities but also risks and threats. These are discussed in the following subsection.

2.10.4.1 Main current threats and challenges

Exponential increase in the number of satellites. The technology to manufacture and launch low-cost, small satellites makes it possible to launch large constellations. This opportunity is being picked up in particular by the commercial sector. Constellations of hundreds of small satellites are expected to be used for Earth observation and constellations of thousands of satellites for communication. This will exacerbate the problems of congestion in orbits and frequencies and of space debris.

Congestion in popular orbits. Although many orbits can be used, some are more in demand than others. Much used orbits include the lowest possible ones, where atmospheric drag is not an issue and which are sun-synchronous, as well as geostationary orbits, which are limited to a fixed height above the equator. There is probably enough space for a lot of satellites, but coordination will be needed to prevent collisions in orbit and when bringing satellites into orbit or otherwise moving them around (space traffic management).

Space debris. This is made up of orbiting objects such as defunct satellites, spent boosters, broken-off parts, solid propellant residues and the results of explosions or collisions of space objects. The last contribute most to the amount of dangerous debris parts. High orbital speeds make even tiny objects very dangerous, as a hit can cause serious or fatal damage. The amount of space debris is increasing, necessitating small orbit

⁽¹⁹³⁾ Council Decision (CFSP) 2015/203 of 9 February 2015 in support of the Union proposal for an international Code of Conduct for outer-space activities as a contribution to transparency and confidence-building measures in outer-space activities, OJ L 33, 10.2.2015, p. 38-44.

⁽¹⁹⁴⁾ United Nations Office for Outer Space Affairs 'Space2030: Space as a driver for peace' (<http://www.unoosa.org/oosa/en/outreach/events/2018/spacetrust.html>).

changes for manoeuvrable satellites from time to time, and may even lead to certain popular orbits becoming unusable.

Space objects crashing to Earth. Although most objects and debris that re-enter the atmosphere burn up, some large objects may hit the ground. The precise crash site can be hard to predict, and sometimes the re-entry comes as a surprise. This probably does not add much to the daily risks faced by the average person, but it creates bad publicity.

Near-Earth objects. These are asteroids and comets that come close to Earth. The possibility that a big NEO could hit our planet is an omnipresent natural risk with a low probability but a high impact. This realisation has led to activities involving searching for and tracking NEOs. However, how to avert an impending collision once it has been predicted is still ascertained.

Space weather. Solar activity in the form of strong flares or eruptions may not only hurt astronauts or damage or deactivate satellites — leading, for example, to loss of GNSS functionality — but also damage power and communications lines on Earth and pose a danger to air travellers.

SST and SSA capability. To give forewarning against impending collisions, the larger space objects are being tracked, and their near-future positions are predicted (SST). However, tracking and prediction capabilities are limited, while the number of potentially dangerous objects is growing. SSA also encompasses, besides SST, the monitoring of NEOs and space weather. As with SST, the current monitoring capacity for NEOs and space weather is not sufficient to cover the risks.

Sensitivity of some satellite positions. Nations that deploy military and strategic satellites want to keep their exact positions secret for protection. This may increase the risk of collisions and may interfere with full support, data exchange and cooperation on SST.

Sensitivity of in-orbit servicing. Even very expensive satellites have a limited lifetime, as some consumables such as propellant or coolant will run out, or malfunctions or damage will occur. This could be remedied by in-orbit servicing as a cheaper alternative to launching a new satellite. Only in recent years has in-orbit servicing become practically and economically conceivable. However, the capacity to approach a satellite and tamper with it poses a risk in particular to military and strategic satellites. For that reason, developments in this direction may be discouraged.

Radio spectrum conflicts. The available bandwidth for radiofrequency communications is limited, and demand threatens to exceed supply. Not only do satellites compete for the same frequency bands, but also terrestrial radiofrequency use can interfere with bands allocated for satellites, for example in the case of ground-based radars and wireless local area networks that operate on the frequencies of the EU's Sentinel-1 satellite, or radar and terrestrial very high-frequency communications that operate in the Automatic Identification System bands received by satellites.

Geopolitical forces frustrate international agreements. Agreements on the use of space need by nature to be international, voluntary and global. Although the UN has had considerable success in establishing such agreements, the current exponential growth in the use of space means that updates to the international agreements are required. Progress is currently slow because of geopolitical issues.

Export control. Whereas growing a space manufacturing and service industry that is globally competitive is an economic goal of the EU, some advanced products and applications may be deemed too sensitive to export outside the EU. This applies in particular to military and dual-use technologies and may restrict global growth opportunities for EU industry.

Supply chain security. Satellites, launchers and all their building blocks work with a number of critical components and materials and are put together using advanced technologies. Access to and control over these should be secured. This means guaranteed access to some basic materials such as rare earth metals, but it also means retaining control over critical companies in the supply chain — companies that often have international shareholders.

Cyber and communications security. The software that runs satellites can be hacked by malicious cyber-tools that can be inserted at any stage in the operation or the production of the satellite or its components. Cyberattacks and cybercrime have become a serious daily issue on Earth and are a realistic threat to space assets as well. In addition, the communications links between satellites and ground receivers can be disrupted by jamming, spoofing or eavesdropping (unintentional radiofrequency interference has been mentioned above).

Security of the ground component. (Civilian) ground stations are not extensively protected against disruption. All space operations and services depend on terrestrial communications links, including the internet, which are targets for cyber- and physical attacks. Jamming, spoofing and eavesdropping are also threats relating to these links.

Increasing use of space for military purposes. Just as civilian use of space is increasing, so is military use. The United States in particular but also Russia have historically been major military space users. Now, China, India, Canada and Australia are also building up capabilities. European countries, too, deploy military and dual-use satellites. Even the EU has started discussing the combination of space and defence activities. Defence capabilities, on Earth or in space, may contribute to global stability, so military use of space is not per se undesirable. However, a wasteful arms race should be avoided.

Development of anti-satellite weapons. In the classic paradigm, a space asset was untouchable. Now, however, capabilities have been developed and are being further developed that can take out satellites. Anti-satellite weapons include manoeuvrable satellites, precision-guided kinetic projectiles, explosives, directed energy and nuclear electromagnetic pulses. New developments include rail guns, high-power lasers, and high-energy microwaves and radiofrequencies. These are weapons that have a low operational cost (a low 'cost per shot') and can be used from the ground or in space to target space assets. Laser and microwave weapons can be used in different degrees, from merely dazzling at low power to disrupting certain functions at medium power and destroying the target at high power.

Inability to attribute outages of space assets to a cause. When a satellite unexpectedly stops functioning, the cause is often unknown. It can be hardware or software malfunction, the result of a hit by a cosmic ray or by space debris, or the result of an attack. Even if a malicious cause is strongly suspected, the question is, 'Who did it?' Today, there is little means of finding this out, and that contributes to impunity, uncertainty and potential instability.

Equitable access to space. As space (including radiofrequency space) is becoming congested, latecomers may find the best places taken. This can put developing countries in particular at a disadvantage.

2.10.4.2 Main current opportunities

Technological advancements and consequent lowering of costs. These are the main drivers in the current increase in space actors, making space accessible for ever more countries and operators. Size and weight are what makes a launch expensive, so miniaturisation (made possible by technological advancements) is a big contributor to reducing launch costs. The use of commercial off-the-shelf parts leads to cost savings, as does standardisation on the basis of the cubesat model (elements measuring 10 cm × 10 cm × 10 cm). Recent success in the development of reusable launchers will also help to save costs.

More private actors. Private commercial firms are starting to offer products and services that were hitherto only provided by governments. While communication and Earth observation have a longer commercial history, commercial services in space tourism, SSA, in-orbit servicing, launch organisation, electronics intelligence (which used to be exclusively a defence activity) and extraterrestrial exploration are now also on offer.

Increasing economic and societal benefits. The increased use of space will be to the benefit of more people, benefiting both consumers and industry. The growth of the space industry itself, and a shift from upstream (systems) to downstream (service provision), will be accompanied by growth in the economy thanks to the use of the new space-based services. Although this will contribute to the congestion in space (orbits, frequencies), it will also create more parties that have an interest in keeping the use of space sustainable.

Availability of funds. Recent decades have seen extreme capital build-up by some countries and individuals. Some of these — private persons as well as countries — spend this capital on space programmes for idealistic reasons or to pursue a long-term vision. Others make it available as venture capital that finances start-up companies in space.

Increased resilience due to many systems. The trend away from a few powerful, expensive satellites and towards constellations of small, inexpensive ones will lead to more resilience to outage of single satellites. Similarly, more independent systems and service providers will lead to less vulnerability, and the interoperability of GNSS will provide more reliable PNT services. In addition, the 'responsive space' concept is

gaining ground; this refers to being able to create functionality in space quickly, including by quickly replenishing outed satellites.

New means of communication. Laser is a way of communicating between two points with a high bandwidth, securely and without disturbing other communications links. This technology can alleviate the problems of radiofrequency spectrum congestion. Satellite-to-satellite communication is easier than satellite–Earth communication by laser, because the latter is hindered by the atmosphere. In addition, quantum communications are being pursued as a promising means of achieving highly secure communications, and the very first trials involving satellite have been done by China.

Increased recognition of space debris and orbit congestion. Both regulators and operators have started to recognise this issue more widely. Regulators are considering guidelines for operators, and the latter are even asking for them. Such guidelines would cover, for example, the obligation to de-orbit satellites at the end of their lifetime to free up orbit space and prevent future collisions. Furthermore, special missions to clean up debris are being considered, although this is a technological challenge. More countries are taking up SST activities, in addition to the United States, and international cooperation in this area is growing. In addition, commercial operators are starting to offer SST services and de-orbiting services. Space traffic management is starting to be considered in international forums.

Increased recognition of the space weather threat. Governments are starting to take up the space weather threat to a greater extent, in the context of increasing resilience and protecting critical infrastructures. International cooperation mechanisms are being considered, for example under the aegis of the UN Committee on the Peaceful Uses of Outer Space / the UN Office for Outer Space Affairs.

International scientific cooperation. While current geopolitical issues are blocking some progress on international agreements, scientific cooperation is continuing, for example on the ISS and for proposed extra-terrestrial missions.

International coordination and governance. There is a significant and growing number of international coordination forums that work on space (and security): not only is there already a series of sub-organs under the UN, but also outside the UN there is a plethora of government, NGO and industry associations. The UN and others are continuing to try to strengthen international governance in order to promote security and sustainability, through various binding and non-binding agreements.

Dual use. If the militarisation of space can be avoided, it will save much cost and risk. Nonetheless, defence was one of the first uses of space by the superpowers, and civil applications have in the end benefited much from military developments. While in Europe there is much less military use of space than, for example, by the United States, there is already experience with dual-use observation satellites, and this model could lead in the future to cost savings and increased efficiency. Furthermore, some of the new types of weapons could conceivably be used to neutralise space debris or protect against an NEO on a collision course.

Near space. Although not quite space, the stratosphere is an attractive domain in which to place vehicles for long persistence. Technologies to make lightweight materials and to collect solar energy are starting to bring this within reach. This technology is referred to as ‘near-space platforms’, ‘high-altitude platforms’ or ‘high-altitude pseudo-satellites’. Stratospheric platforms for Earth observation or for communication have the advantage of being able to remain stationary over a location, but at an altitude of tens of kilometres, as opposed to a 36 000 km altitude for a classical geostationary satellite. Persistence makes it possible to continuously monitor movements (which cannot be done with low-orbital satellites), while close range allows much higher spatial resolution than from geostationary orbit.

2.10.4.3 The European Union’s position

The Commission aims to position the EU for the next 7 years (2021–2027, the period of the next MFF) with an overarching EU space programme⁽¹⁹⁵⁾. It seeks to continue major EU investments in global positioning and navigation and in Earth observation through Galileo/EGNOS and Copernicus, respectively. It proposes new activities in satellite communications for government users while responding to challenges relating to SSA, although these two aspects will be pursued with much more limited investments through an approach of pooling Member State-level resources, as opposed to building up EU-level assets.

⁽¹⁹⁵⁾ European Commission, ‘Proposal for a Regulation establishing the space programme of the Union and the European Union Agency for the Space Programme and repealing Regulations (EU) No 912/2010, (EU) No 1285/2013, (EU) No 377/2014 and Decision 541/2014/EU’ (COM(2018) 447 final), Brussels, 6.6.2018.

The proposed space programme also emphasises the development of the space economy, the security aspects of space and the autonomy of Europe. To turn to security, the development of the Copernicus Security Service is already being addressed through studies and workshops. Of the Copernicus services, it is one of the last to have been developed, and its use is likely to grow among civil security users, and possibly also among military users, although it will remain a civil-driven service.

With regard to autonomy, there is particular emphasis on the autonomy of access to space. Nowadays, many European satellites are launched by Russian, Indian and US launchers. This can be economically advantageous, but the EU should not depend on them (it should have its own alternatives); furthermore, the EU launch industry needs a large market in order to be viable.

The Commission is proposing an increase in its framework R & D programme for the next MFF (Horizon Europe; see Section 3.1.8). Part of that budget will be earmarked for research on space and on security.

The EU is reinforcing its position in defence, and one important ingredient is the European Defence Fund (EDF) for defence R & D, also proposed for the next MFF. The links between space and defence have been highlighted in recent political statements. The EDF may conceivably also provide funding for space-related projects.

With regard to the longer term, European leaders have voiced some far-reaching visions on space. For example, in a recent speech ⁽¹⁹⁶⁾ Commissioner Bieńkowska mentioned the notions of a collective European objective in space involving space exploration, of a European space council and of a European space force.

2.10.5 Stakeholders

2.10.5.1 European Union stakeholders

In the EU, political directions, policies, strategies, regulations and decisions in space and security are made at the usual various levels of the European Council, the Council of the European Union, the European Parliament and the Commission. In addition to those, the following stakeholders have been identified.

Council Working Party on Space

The Council Working Party on Space handles work on the development of the European space policy and the related legislation. This includes the development of Copernicus, SST, relations with the ESA and EU international relations in space.

<http://www.consilium.europa.eu/en/council-eu/preparatory-bodies/working-party-space/>

European Union Military Committee

The committee is the supreme military body of the Council of the EU, composed of the chiefs of defence of the Member States. It directs all military activities in the context of the EU, in particular the planning and execution of military missions and operations under the CSDP and the development of military capabilities. It has an interest in Earth observation, navigation and the use of space to support military missions and intelligence.

<http://www.consilium.europa.eu/en/council-eu/preparatory-bodies/european-union-military-committee/>

European Commission Directorate-General for Internal Market, Industry, Entrepreneurship and SMEs

This is the Commission DG responsible for EU policy on the single market, industry, entrepreneurship and small businesses. Key requirements are related to: Development of Copernicus – The European Earth Observation Programme; EGNOS – The European Geostationary Navigation Overlay Service; and Galileo – The Global Satellite Navigation System (GNSS) for further use in the security and defence.

<http://ec.europa.eu/growth/>

⁽¹⁹⁶⁾ Opening speech at the 11th Annual Conference on European Space Policy, Brussels, 22 January 2019 (<https://www.spaceconference.eu/downloads/2019/ESPI-proceedings-11th-European-Space-Policy-Conference.pdf>).

European Commission Directorate-General for Communications Networks, Content and Technology

Connect is responsible for the Commission's policies to create a digital single market, with key areas of responsibility such as data, cybersecurity and copyright. It has interests in secure communication and cybersecurity.

https://ec.europa.eu/info/departments/communications-networks-content-and-technology_en

European Commission Directorate-General Joint Research Centre

The JRC is the European Commission's science and knowledge service. It has solid research and policy support experience, developed in house, as well as broad networks with academia, industry, Member States and city authorities.

Key space-related areas of its research are Earth observation; integrated maritime surveillance; emergency preparedness, response, disaster risk management and resilience in cases of natural and man-made hazards; the fight against crime and terrorism, including combating the illicit trafficking of people, drugs and weapons; cybersecurity, data protection and space infrastructures, as well as the use of communications data by security and intelligence agencies; technical aspects relating to the implementation of treaties and conventions on the non-proliferation of nuclear, chemical and biological weapons; and support for studies on the implications of demographic change, and the root causes, likely scale, timing and impact of migration. See Section 3.4 for more details. <https://ec.europa.eu/jrc/en>

European Commission European Political Strategy Centre

The European Political Strategy Centre is the European Commission's in-house think tank. It provides strategic analysis, advice and support to the President and the Commission. Tasked with a mission to innovate and disrupt, the centre provides the President and the College of Commissioners with strategic, evidence-based analysis and forward-looking policy advice.

https://ec.europa.eu/epsc/home_en

European Commission: user DGs

Within the Commission, a number of DGs make use of space services to implement their security-related policies or to have their policies implemented by agencies. These are primarily:

- DG Migration and Home Affairs — internal security, border security, migration;
- DG Maritime Affairs and Fisheries, DG Mobility and Transport — maritime security and safety;
- DG Taxation and Customs Union, DG Trade — customs, dual-use exports;
- ECHO — disaster response, humanitarian aid;
- DG International Cooperation and Development — international development, cooperation and aid;
- Service for Foreign Policy Instruments — operational EU foreign policy, crisis and security support to non-EU countries, enforcing EU sanctions.

https://ec.europa.eu/info/departments_en

Research Executive Agency

This is the European Commission's funding body for research and innovation. It manages EU research grants, including for space-related projects.

http://ec.europa.eu/info/departments/research-executive-agency_en

European GNSS Agency

The GSA manages Europe's GNSS programmes, Galileo and EGNOS. Its interest is in furthering their development and uptake.

<https://www.gsa.europa.eu/>

European Border and Coast Guard Agency (Frontex)

Frontex promotes, coordinates and develops European border management. It helps EU Member States and Schengen associated countries to manage their external borders, as well as to harmonise border controls

across the EU. It facilitates cooperation between the border authorities in the EU Member States, providing technical support and expertise. It runs the border surveillance component of the Copernicus Security Service, to provide information to itself and to Member State border authorities.

<https://frontex.europa.eu/>

European Maritime Safety Agency

EMSA provides technical expertise and operational assistance to improve maritime safety, pollution preparedness and response, and maritime security. It also offers maritime services such as Earth observation. It runs the maritime surveillance component of the Copernicus Security Service, to provide information to European maritime security users, such as Frontex, the European Fisheries Control Agency, Europol and the Maritime Analysis and Operations Centre — Narcotics, and to Member State authorities.

<http://www.emsa.europa.eu/>

European Fisheries Control Agency

This EU agency promotes the highest common standards for control, inspection and surveillance under the common fisheries policy. It makes use of ship detection and tracking through satellite communications and satellite imaging.

<https://www.efca.europa.eu>

European Union Agency for Law Enforcement Cooperation (Europol)

Europol is the law enforcement agency of the EU supporting Member States in their fight against terrorism, cybercrime and other serious and organised crime. It has an interest in space assets for policing operation support, secure communication, Earth observation and image analysis, intelligence and cybersecurity.

<https://www.europol.europa.eu/>

European External Action Service

The EEAS is the diplomatic service and foreign and defence ministry of the EU, helping the HR/VP to implement the EU's CFSP. Its interest in space relates to surveillance and reconnaissance for military/security operations, satellite communications, autonomous access to space, permanent earth observation and cybersecurity. It aims to make use of the full potential of Copernicus and of the European GNSS for security purposes.

<http://eeas.europa.eu>

EEAS European Union Military Staff

The Military Staff is a Directorate-General of the EEAS that contributes to the EU's CSDP by providing strategic advice to the HR/VP and commanding non-executive operations through its military planning and conduct capability operational headquarters. Its interest in space relates to early warning, situation assessment, strategic planning for military operations, communications and information systems, concept development, and training and education.

http://eeas.europa.eu/headquarters/headquarters-homepage/5436/european-union-military-staff-eums_en?page=1

European Defence Agency

The EDA supports the development of defence capabilities, military cooperation, defence R & T and the defence industry. Among its priorities are the preparatory action on defence research (PADR), the updating of the capability development plan, the Coordinated Annual Review on Defence, and key capability programmes governmental satellite communications. It is interested in further development of the next generation of European space systems, taking into account their potential for dual use, and supports initiatives on SST, governmental satellite communications, the use of Galileo for security purposes, Earth observation and imagery analysis, secure communications and data transmission, countering cyberthreats (cyberdefence), maritime patrolling and escorting naval surveillance systems, enhanced battlespace information and communication services, and space-based information services.

<https://www.eda.europa.eu/>

European Union Satellite Centre

SatCen supports the decision making and actions of the EU in the field of the CFSP, in particular the CSDP, including EU crisis management missions and operations, by providing products and services resulting from the exploitation of relevant space assets and collateral data, including satellite imagery and aerial imagery, and related services. It has interests in Earth observation and navigation, humanitarian and civil protection missions, security and military surveillance/intelligence, protection of space infrastructures, secure communications and SSA.

<https://www.satcen.europa.eu/>

European Union Institute for Security Studies

The EUISS is the EU agency dealing with the analysis of foreign, security and defence policy issues. It supports the development of the CSDP through outreach activities and expert publications. It has interests in cybersecurity, independent space infrastructures, improving space system resilience, reducing external dependency, and ensuring a secure and sustainable environment for outer space activities.

<https://www.iss.europa.eu/>

Emergency Response Coordination Centre

The Emergency Response Coordination Centre, operating within ECHO, was set up to support a coordinated and quicker response to disasters both inside and outside Europe, using resources from the countries participating in the EU's Civil Protection Mechanism. Use of space for analyses of real-time information on disasters; monitoring hazards; preparing plans for the deployment of experts, teams and equipment; mapping available assets and coordinating the EU's disaster response efforts by matching offers of assistance to the needs of the disaster-stricken country; and better planning will further enhance the centre's capacity for rapid response.

https://ec.europa.eu/echo/what/civil-protection/emergency-response-coordination-centre-ercc_en

European Space Agency

The ESA is an intergovernmental organisation with 22 member states, dedicated to the exploration of space. Established in 1975, it has a staff of about 2 200 and an annual budget of about EUR 5.7 billion (in 2019). The ESA's space flight programme includes the launch and operation of unmanned exploration missions to other planets and the Moon; Earth observation, science and telecommunication; operating and developing launchers with industry; and maintaining a major spaceport, the Guiana Space Centre at Kourou, French Guiana. The ESA has headquarters in Paris and facilities in Noordwijk, the Netherlands; Frascati, Italy, Darmstadt, Germany; Cologne, Germany; Harwell, the United Kingdom; and Villanueva de la Cañada, Madrid, Spain.

<http://www.esa.int>

ESA SSA Space Weather Coordination Centre

The ESA's SSA Space Weather Coordination Centre is operated by a Belgian consortium on behalf of the Agency's SSA Programme Office. It has the responsibility for overall coordination of the space weather asset network (in partnership with several expert service centres), maintenance of the associated ESA applications and monitoring of the system.

https://www.esa.int/Safety_Security/About_the_Space_Weather_Coordination_Centre

2.10.5.2 International stakeholders

UN Office for Outer Space Affairs

This UN body works to promote international cooperation on the peaceful use and exploration of space, and on the use of space science and technology for sustainable economic and social development. It assists UN member states to establish legal and regulatory frameworks to govern space activities and strengthens the capacity of developing countries to use space science technology and applications for development.

<http://www.unoosa.org/>

UN Committee on the Peaceful Uses of Outer Space (COPUOS)

The committee was set up by the UN General Assembly to govern the exploration and use of space for the benefit of all humanity for peace, security and development. It is tasked with reviewing international cooperation on peaceful uses of outer space, studying space-related activities that could be undertaken by the UN, encouraging space research programmes and studying legal problems arising from the exploration of outer space. There are two subsidiary bodies: the Scientific and Technical Subcommittee and the Legal Subcommittee.

<http://www.unoosa.org/oosa/en/ourwork/copuos/index.html>

International Committee on Global Navigation Satellite Systems

The committee promotes voluntary cooperation on matters of mutual interest related to civil satellite-based PNT. It encourages coordination among GNSS providers and regional systems, as well as improvements to ensure greater compatibility, interoperability and transparency, and it carries out activities to promote the introduction and use of these services.

<http://www.unoosa.org/oosa/en/ourwork/icg/icg.html>

International Telecommunication Union

This is the UN's specialised agency for ICT. It allocates global radio spectrum and satellite orbits, and develops the technical standards that ensure networks and technologies seamlessly interconnect.

<https://www.itu.int/>

2.10.6 Legislation and reference documents

EU legislation and reference documents

- European Commission, 'White Paper: space — a new European frontier for an expanding Union: an action plan for implementing the European space policy (COM(2003) 673 final), Brussels, 11 November 2003.
- European Council, *European Security Strategy: A secure Europe in a better world*, 12 December 2003.
- European Commission and European Space Agency (2004), Framework agreement between the European Community and the European Space Agency (L 261/64), Brussels, 6 August 2004.
- European Parliament Resolution 2004/2171(INI) on security research — the next steps, Brussels, 23 June 2005.
- European Commission, Commission communication, 'European space policy' (COM(2007) 212 final), Brussels, 26 April 2007.
- European Space Agency, Resolution on the European space policy (ESA BR 269), 22 May 2007.
- European Parliament Resolution 2008/2030(INI) on space and security, Strasbourg, 10 July 2008.
- Council Resolution of 26 September 2008, 'Taking forward the European Space Policy', *OJ C 268*, 23.10.2008, p. 1-6.
- European Parliament Resolution P6_TA(2008)0564 on the European space policy: how to bring space down to earth, Strasbourg, 20 November 2008.
- Regulation No (EU) 911/2010 of the European Parliament and of the Council of 22 September 2010 on the European Earth monitoring programme (GMES) and its initial operations (2011 to 2013), *OJ L 276*, 20.10.2010, p. 1-10.
- Regulation (EU) No 912/2010 of the European Parliament and of the Council of 22 September 2010 setting up the European GNSS Agency, repealing Council Regulation (EC) No 1321/2004 on the establishment of structures for the management of the European satellite radio navigation programmes and amending Regulation (EC) No 683/2008, *OJ L 276*, 20.10.2010, p. 11-21.
- European Commission, Commission communication, 'The EU internal security strategy in action: five steps towards a more secure Europe' (COM(2010) 673 final), Brussels, 22 November 2010.
- Council of the European Union and Council of the European Space Agency, 7th Space Council Resolution, 'Global challenges: taking full benefit of European space systems', Brussels, 25 November 2010.

- European Commission, Commission communication, 'Towards a space strategy for the European Union that benefits its citizens' (COM(2011) 152 final), Brussels, 4 April 2011.
- European Commission, Commission communication, 'Establishing appropriate relations between the EU and the ESA' (COM(2012) 671 final), Brussels, 14 November 2012.
- European Commission, Commission communication, 'EU space industrial policy: releasing the potential for economic growth in the space sector' (COM(2013) 108 final), Brussels, 28 February 2013.
- European Commission, Commission communication, 'Towards a more competitive and efficient defence and security sector' (COM(2013) 542 final), Brussels, 24 July 2013.
- Regulation (EU) No 1285/2013 of the European Parliament and of the Council of 11 December 2013 on the implementation and exploitation of European satellite navigation systems and repealing Council Regulation (EC) No 876/2002 and Regulation (EC) No 683/2008 of the European Parliament and of the Council, OJ L 347, 30.12.2013, p. 1-24.
- High Representative of the Union for Foreign Affairs and Security Policy, *Final Report by the High Representative/Head of the EDA on the common security and defence policy*, Brussels, 15 October 2013.
- European Commission, Commission report, *Progress report on establishing appropriate relations between the European Union and the European Space Agency (ESA)* (COM(2014) 56 final), Brussels, 6 February 2014.
- EEAS, International Code of Conduct for Outer Space Activities (draft), 31 March 2014 ⁽¹⁹⁷⁾.
- Regulation (EU) No 377/2014 of the European Parliament and of the Council of 3 April 2014 establishing the Copernicus Programme and repealing Regulation (EU) No 911/2010, OJ L 122, 24.4.2014, p. 44-66.
- Regulation (EU) No 512/2014 of the European Parliament and of the Council of 16 April 2014 amending Regulation (EU) No 912/2010 setting up the European GNSS Agency, OJ L 150, 20.5.2014, p. 72-92.
- Decision No 541/2014/EU of the European Parliament and of the Council of 16 April 2014 establishing a framework for space surveillance and tracking support, OJ L 158, 27.5.2014, p. 227-234.
- European Commission, Commission communication, The final implementation report of the EU Internal Security Strategy 2010-2014 (COM(2014) 365 final), Brussels, 20 June 2014.
- Council Decision 2014/401/CFSP of 26 June 2014 on the European Union Satellite Centre and repealing Joint Action 2001/555/CFSP on the establishment of a European Union Satellite Centre, OJ L 188, 27.6.2014, p. 73-84.
- European Commission, Commission implementing decision on the procedure for participation of the Member States in the Space Surveillance and Tracking Support Framework (C(2014) 6342 final), Brussels, 12 September 2014.
- Council Decision (CFSP) 2015/203 of 9 February 2015 in support of the Union proposal for an international Code of Conduct for outer-space activities as a contribution to transparency and confidence-building measures in outer-space activities, OJ L 33, 10.2.2015, p. 38-44.
- European Commission, Commission communication, 'The European agenda on security' (COM(2015) 185 final), Strasbourg, 28 April 2015.
- Council of the European Union, draft Council conclusions on the renewed European Union internal security strategy 2015-2020 (9798/15), Brussels, 10 June 2015.
- European Parliament Resolution 2015/2276(INI) on space capabilities for European security and defence, Strasbourg, 8 June 2016.
- European Parliament Resolution 2016/2731(RSP) on space market uptake, Strasbourg, 8 June 2016.
- EEAS (2016), 'Shared vision, common action: a stronger Europe — A global strategy for the European Union's foreign and security policy', 10715/16, June 2016.
- European Union and European Space Agency, *Joint statement on shared vision and goals for the future of Europe in space*, Brussels, 26 October 2016.

⁽¹⁹⁷⁾ https://eeas.europa.eu/sites/eeas/files/space_code_conduct_draft_vers_31-march-2014_en.pdf

- European Commission, Commission communication, 'Space strategy for Europe' (COM(2016) 705 final), Brussels, 26 October 2016.
- High Representative of the Union for Foreign Affairs and Security Policy, *Implementation Plan on Security and Defence* (14392/16), Brussels, 14 November 2016.
- European Commission, Commission communication, 'European defence action plan' (COM(2016) 950 final), Brussels, 30 November 2016.
- European Space Agency, *Towards Space 4.0 for a United Space in Europe*, Lucerne, 2 December 2016.
- European Commission Decision C(2016) 8482 on a coordination plan for the space surveillance and tracking support framework and on the procedure for the participation of Member States, Brussels, 19 December 2016 (not public).
- Council of the European Union, Council conclusions on progress in implementing the EU global strategy in the area of security and defence (6875/17), Brussels, 6 March 2017.
- European Commission, Commission communication, 'Launching the European Defence Fund' (COM(2017) 295 final), Brussels, 7 June 2017.
- European Commission, 'Reflection paper on the future of European defence' (COM(2017) 315 final), Brussels, 7 June 2017.
- European Commission, 'Proposal for a Regulation establishing the European Defence Industrial Development Programme aiming at supporting the competitiveness and innovative capacity of the EU defence industry' (COM(2017) 294 final), Brussels, 7 June 2017.
- Council Decision 14866/17 establishing permanent structured cooperation (PESCO) and determining the list of participating Member States, Brussels, 8 December 2017.
- European Commission, Commission report on the implementation of the space surveillance and tracking (SST) support framework (2014-2017) (COM(2018) 256 final), Brussels, 3 May 2018.
- European Commission, 'Proposal for a Regulation establishing the space programme of the Union and the European Union Agency for the Space Programme and repealing Regulations (EU) No 912/2010, (EU) No 1285/2013, (EU) No 377/2014 and Decision 541/2014/EU' (COM(2018) 447 final), Brussels, 6 June 2018.
- European Commission, 'Proposal for a Regulation establishing Horizon Europe — the Framework Programme for Research and Innovation, laying down its rules for participation and dissemination' (COM(2018) 435 final), Brussels, 7 June 2018.
- European Commission, 'Proposal for a Regulation establishing the Internal Security Fund' (COM(2018) 472 final), Brussels, 13 June 2018.
- European Commission, 'Proposal for a Regulation establishing the European Defence Fund' (COM(2018) 476 final), Brussels, 13 June 2018.

UN General Assembly legislation and reference documents

Treaties (T) and resolutions (R) at the level of the UN General Assembly (see also UN Office for Outer Space Affairs, 2017).

Item		Date	Ref	Link
Declaration of Legal Principles Governing the Activities of States in the Exploration and Use of Outer Space	R	13.12.1963	1962 (XVIII)	http://www.unoosa.org/oosa/en/ourwork/spacelaw/principles/legal-principles.html
Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies	T	19.12.1966	RES 2222 (XXI)	http://www.unoosa.org/oosa/en/ourwork/spacelaw/treaties/introouterspacetreaty.html
Agreement on the Rescue of Astronauts, the Return of Astronauts and the Return of Objects Launched into Outer Space	T	19.12.1967	RES 2345 (XXII)	http://www.unoosa.org/oosa/en/ourwork/spacelaw/treaties/introrescueagreement.html

Item		Date	Ref	Link
Convention on International Liability for Damage Caused by Space Objects	T	29.11.1971	RES 2777 (XXVI)	http://www.unoosa.org/oosa/en/ourwork/spacelaw/treaties/introliability-convention.html
Convention on Registration of Objects Launched into Outer Space	T	12.11.1974	RES 3235 (XXIX)	http://www.unoosa.org/oosa/en/ourwork/spacelaw/treaties/introregistration-
Agreement Governing the Activities of States on the Moon and Other Celestial Bodies	T	05.12.1979	RES 34/68	http://www.unoosa.org/oosa/en/ourwork/spacelaw/treaties/intromoon-agreement.html
Principles Governing the Use by States of Artificial Earth Satellites for International Direct Television Broadcasting	R	10.12.1982	RES 37/92	http://www.unoosa.org/oosa/en/ourwork/spacelaw/principles/dbs-principles.html
Principles Relating to Remote Sensing of the Earth from Outer Space	R	03.12.1986	RES 41/65	http://www.unoosa.org/oosa/en/ourwork/spacelaw/principles/remote-sensing-
Principles Relevant to the Use of Nuclear Power Sources In Outer Space	R	14.12.1992	RES 47/68	http://www.unoosa.org/oosa/en/ourwork/spacelaw/principles/nps-principles.html
Declaration on International Cooperation in the Exploration and Use of Outer Space for the Benefit and in the Interest of All States, Taking into Particular Account the Needs of Developing Countries	R	13.12.1996	RES 51/122	http://www.unoosa.org/oosa/en/ourwork/spacelaw/principles/space-benefits-declaration.html
Transparency and confidence-building measures in outer space activities	R	05.12.2013	RES 68/50	http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/68/50

Source: Authors.

2.11 Defence

Traditionally, internal and external security have been considered separately, conceptually and practically. However, in recent years the dividing lines have been fading, presenting a huge challenge for the design of security policies and the institutions safeguarding it.

Having its origin in the Treaty of Maastricht of 1992, the EU security policy is split between the CFSP and the justice and home affairs policy ⁽¹⁹⁸⁾. Whereas both policies contain significant components relating to internal and external security, the justice and home affairs policy covers migration and asylum policy, judicial cooperation and criminal law, and policy cooperation, while the CFSP deals mainly with external security and military policy.

The CFSP includes the European security and defence policy (ESDP), the main objectives of which are military and civilian crisis management operations, including response to natural, humanitarian or other disasters. Since 2003, the EU has deployed international interventions and missions within the ESDP framework.

The origin of the ESDP dates back to the British-French Summit in Saint Malo in 1998, when the two states called for a European foreign policy that would allow Europe to fulfil its role on the global stage, including with regard to defence and security issues. For that purpose, the EU needed the capacity for autonomous action, backed by military forces, to respond to international crises. In 1999, the European Council of Cologne endorsed this view, confirming the ESDP role and setting out its goals ⁽¹⁹⁹⁾.

2.11.1 The European Security Strategy (2003)

In 2003, the US military action in Iraq without a mandate from the UN and with the support of some EU Member States, while the EU's common position was being drafted, created an internal EU crisis of confidence (Bailes, 2005). As a consequence, that same year the High Representative for the CFSP, Javier Solana, presented the first European security strategy, 'A secure Europe in a better world' (European Council, 2003), adopted by the European Council in December 2003.

⁽¹⁹⁸⁾ The Maastricht Treaty changed the former European treaties and created a European Union based on three pillars: the European Communities, the CFSP, and cooperation in the field of justice and home affairs.

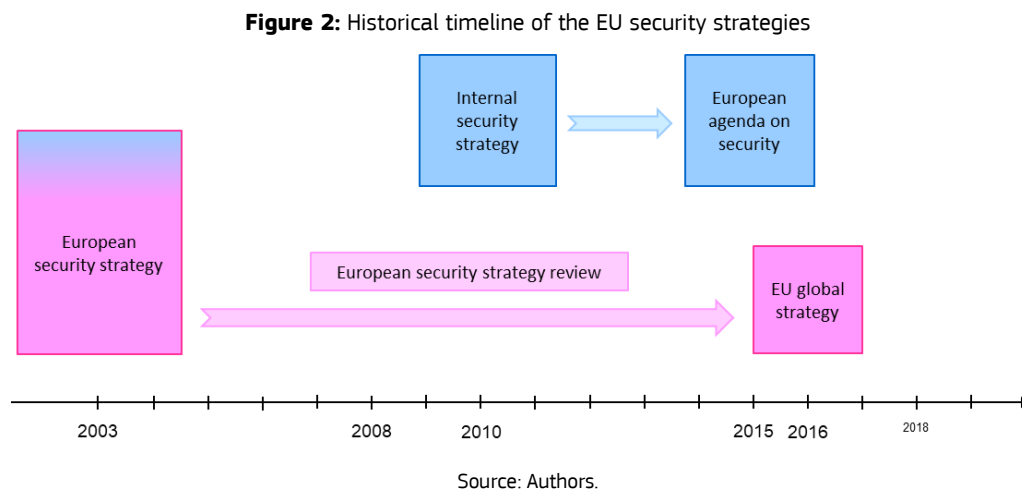
⁽¹⁹⁹⁾ EDA, 'Inception' (<https://www.eda.europa.eu/Aboutus/our-history/inception>).

This strategy defined for the first time the EU's security environment, identifying a number of challenges to Europe's internal and external security related to the connected threats of terrorism, the proliferation of weapons of mass destruction, regional conflicts, failing states and organised crime. It provided a conceptual framework for the CFSP, including what would later become the CSDP ⁽²⁰⁰⁾.

In 2004, the European Council created as a complement to the security strategy the EDA, an intergovernmental agency to be active in the field of developing defence capabilities, research, acquisitions and armaments.

In December 2007, the Council of the European Union invited the SG/HR (with the European Commission and the Member States) to examine the implementation of the European security strategy ⁽²⁰¹⁾ with a view to improving it and proposing elements to complement it. A year later, *Report on the implementation of the European security strategy: Providing security in a changing world* (European Union, 2008) was published, reinforcing the strategy and identifying new security threats, such as cybersecurity, energy security and climate change. It also called for a greater emphasis on a more effective and capable Europe, on engagement with our neighbourhoods and on multilateralism.

Figure 2 shows a historical timeline of the EU strategies on security, both external and internal, presented in this chapter.



2.11.2 The European Union internal security strategy (2010)

The 2003 European security strategy looked at the external aspects of Europe's security. In March 2010, the Council of the European Union complemented the strategy by approving an internal security strategy (Council of the European Union, 2010).

The document presented current threats to internal security (i.e. terrorism, serious and organised crime, cybercrime, cross-border crime, violence, and natural and man-made disasters) and the existing activities responding to these challenges; it set out the principles behind the strategy, and finally gave some guidelines for future action.

Later that year, the European Commission adopted a communication on the internal security strategy ⁽²⁰²⁾, which proposed five strategic directions with detailed actions: serious and organised crime, terrorism, cybercrime, border security and natural or man-made disasters. This document also highlighted the global perspective (external dimension) of internal security.

⁽²⁰⁰⁾ The Treaty of Lisbon (signed in 2007 and entered into force in 2009) renamed the European Security and Defence Policy (ESDP) to Common Security and Defence Policy (CSDP). It provided for the creation of the European External Action Service, and the Commission delegations in countries outside the EU became EU delegations.

⁽²⁰¹⁾ Council of the European Union Conclusions 16616/1/07.

⁽²⁰²⁾ European Commission, Commission communication, 'The EU internal security strategy in action: five steps towards a more secure Europe' (COM(2010) 673 final), Brussels, 22.11.2010.

2.11.3 The European agenda on security (2015)

In June 2014, the European Council called on the Commission to review the EU internal security strategy and to update it by mid-2015 ⁽²⁰³⁾. A year later, the Commission presented the European agenda on security ⁽²⁰⁴⁾, which set out a new strategy to tackle security threats in the EU for the period 2015-2020.

The security agenda identifies three priorities for EU action: terrorism and radicalisation, organised crime and cybercrime. It focuses on bringing EU added value by facilitating information exchange between law enforcement authorities and EU agencies, increasing operational police cooperation, and boosting training and co-funding for security at EU-level.

2.11.4 The European Union global strategy (2016)

Based on a mandate from the European Council of December 2014 to prepare an EU global strategy on foreign and security policy, the HR/VP, Federica Mogherini, engaged in a two-step process: an assessment of the EU's challenges and opportunities in the evolving global environment (December 2014-June 2015) and a strategic reflection, in collaboration with the Commission and Member States, resulting in the proposal of an EU global strategy on foreign and security policy (by June 2016).

The new EU global strategy, 'Shared vision, common action: a stronger Europe — a global strategy for the European Union's foreign and security policy' (EEAS, 2016), was presented in June 2016 and replaced the previous European security strategy. It presented five priorities: (1) the security and defence of the Union, (2) state and societal resilience in the EU's eastern and southern neighbourhoods, (3) an integrated approach to conflict and crises, (4) cooperative regional orders and (5) global governance.

Soon after the strategy was launched in November 2016, the HR/VP presented an implementation plan (High Representative of the Union for Foreign Affairs and Security Policy, 2016), which set out proposals to implement the strategy in the area of security and defence. It aimed to deepen defence cooperation, moving towards a permanent structured cooperation (PESCO); enhance the EU's military and civilian response tools; improve the planning and conduct of missions; and enhance CSDP partnerships with non-EU countries. The implementation of the strategy is closely monitored and detailed reports are issued annually ⁽²⁰⁵⁾.

In December 2017, PESCO was launched. It stemmed from an opportunity provided by the Lisbon Treaty but never used before. Twenty-five Member States committed, inter alia, to join forces on common projects and to provide troops and assets for common missions and operations.

PESCO complements two other important current initiatives: the EDF, which supports certain collaborative projects, and the Coordinated Annual Review on Defence, which supports Member States' efforts to better identify opportunities for new collaborative initiatives (in particular PESCO projects). The alignment of these initiatives with PESCO and their orientation towards the agreed EU capability development priorities is key to focus the new dynamic in European defence matters on a more coherent European capability landscape and a full-spectrum force package usable for operations and missions.

An initial list of 17 projects to be developed under PESCO was adopted by the Council on 6 March 2018 ⁽²⁰⁶⁾ and a second batch of 17 projects was added on 19 November 2018 ⁽²⁰⁷⁾. The list of these 34 projects, ordered by theme, can be found in Annex 3.

Although PESCO projects are aimed at capability development or operations, and therefore are not R & D projects per se, they are closely related to R & D goals, and the EDF plans to offer more favourable funding if an R & D project contributes to PESCO project goals.

⁽²⁰³⁾ Council of the European Union, Council conclusions EUCO 79/14, Brussels, 27.6.2014.

⁽²⁰⁴⁾ European Commission communication COM(2015) 185 final.

⁽²⁰⁵⁾ EEAS, 'EU global strategy' (<https://europa.eu/globalstrategy/en/news>).

⁽²⁰⁶⁾ Council Decision (CFSP) 2018/340 of 6 March 2018 establishing the list of projects to be developed under PESCO, OJ L 65, 8.3.2018, p. 24-27.

⁽²⁰⁷⁾ Council Decision (CFSP) 2018/1797 of 19 November 2018 amending and updating Decision (CFSP) 2018/340 establishing the list of projects to be developed under PESCO, OJ L 294, 21.11.2018, p. 18-22.

3 Security and defence research

This chapter presents a short history of EU research in security (Section 3.1) and defence (Section 3.2), before reviewing the recent and current research projects funded through the EU Horizon 2020 Framework Programme (Section 3.3). An inventory of relevant projects covering the period 2014-2018 has been carried out, allowing the production of an informative statistical analysis, such as distribution of projects per building block, core priority, Horizon 2020 programme, country involved, etc. As a consequence of the growing overlap between both civil and defence domains, the dual-use nature of projects has also been looked at. This chapter also depicts the specific contribution of the Joint Research Centre to the various building blocks (Section 3.4).

3.1 History and evolution of European Union security research

A graphical overview of the European security research, including advisory bodies, with a timeline is presented in **Figure 7**.

3.1.1 First steps: the Group of Personalities and the preparatory action on security research

The events of 11 September 2001 can be seen as the origin of a paradigm shift in security as it was traditionally understood and implemented in western countries. The threats faced by our modern society involve international terrorism, organised crime, climate change, trafficking of people and goods, and natural disasters. All these phenomena are transnational in nature.

The EU in particular is facing such security challenges, and the threats are multifaceted, complex and interrelated; therefore, a common EU approach relying on strong security research in the EU is needed.

The former dividing lines between internal and external security are increasingly fading, posing an enormous challenge for the design of security policy and the institutions safeguarding it. The first European security strategy, 'A secure Europe in a better world' (European Council, 2003), was adopted by the European Council in 2003. It identified a number of challenges to Europe's internal and external security, related to the connected threats of terrorism, the proliferation of weapons of mass destruction, regional conflicts, failing states and organised crime. The strategy provided the basis for a new European security policy, including a framework for European security-related research.

To complement this security strategy, in 2004 the Council of Ministers decided to create an intergovernmental agency in the field of developing defence capabilities, research, acquisitions and armaments, the EDA ⁽²⁰⁸⁾.

In 2003, the European Commission took the initiative and started the development of a European security research programme (ESRP), setting up a Group of Personalities in the field of security research. It was made up of two commissioners, four members of the European Parliament, and industrialists and security experts from international organisations and research institutes. Its mission was 'to propose principles and priorities of a European Security Research Programme in line with the EU's foreign, security and defence policy objectives' (European Commission, 2004).

In 2004, the Group of Personalities presented its final report, *Research for a Secure Europe* (European Commission, 2004), to the Commission; the report contained a number of recommendations, among which were the creation of an EU-funded ESRP, to be launched in 2007 under FP7, and the establishment of the European Security Research Advisory Board (ESRAB) to draw the strategic lines of action, prepare the ESRP's research agenda and advise on the principles and mechanisms for its implementation.

In February 2004, the Commission launched the first research programme dedicated to security: the preparatory action on the enhancement of the European industrial potential in the field of security research ⁽²⁰⁹⁾. Between 2004 and 2006, EUR 65 million were allocated to support 39 projects across 3 annual calls for proposals.

⁽²⁰⁸⁾ <https://www.eda.europa.eu/>; consulted on 14 December 2018.

⁽²⁰⁹⁾ European Commission, Commission communication, 'Implementation of the preparatory action on the enhancement of the European industrial potential in the field of security research: towards a programme to advance European security through research and technology' (COM(2004) 72 final), Brussels, 3.2.2004.

The purpose of the preparatory action on security research (PASR) was to test the feasibility of a full ESRP within the R & T framework programmes. The Directorate-General for Enterprise and Industry was responsible for its preparation and implementation.

Following the input of the Group of Personalities, the following five themes were defined in the PASR:

1. Theme A — improving situation awareness;
2. Theme B — optimising security and the protection of networked systems;
3. Theme C — protecting citizens from terrorist attacks and CBRN and energetic substances;
4. Theme D — enhancing crisis management;
5. Theme E — achieving interoperability between EU security organisations.

The main objective of the PASR was to develop, demonstrate and validate technological solutions in each of the above themes. Several topics were suggested in the calls, although some degree of flexibility was allowed to enable the applicants to explore broader topics (Centre for Strategy and Evaluation Services, 2011a). The project priorities encouraged included networked systems, protection against terrorism, crisis management, interoperability and integrated systems, and situation awareness.

The main areas of the 39 projects were access control, border control, transport, ICT and surveillance systems and, to a lesser extent, critical infrastructures and CBRN-E protection.

The PASR paved the way and prepared the foundations for a comprehensive ESRP from 2007 onwards under FP7.

In September 2004, the Commission presented the communication 'Security research: the next steps' ⁽²¹⁰⁾, in which it set out the steps to be taken in security research:

- **Developing an ESRP under FP7 (2007-2013).** This was intended to complement Community programmes and security and defence research activities conducted at national and intergovernmental levels.
- **Consultation and cooperation with stakeholders.** The Commission established ESRAB to advise on the content of the ESRP and its implementation. The Commission ensured the coordination of ESRP with international organisations, such as the UN, the OSCE and NATO, and with European organisations such as the ESA.
- **Creating an effective institutional framework.** The Commission ensured that the requirements of the European security strategy, the CFSP and the ESDP were fully taken into account in the development of security research. At the same time, it developed cooperation with the EDA and coordination with other important Commission policies relating to internal security to take them into account when developing security research.
- **Awarding contracts and funding relating to security research.** The Commission put in place effective and flexible mechanisms governing contracts, participation and funding, for example to allow co-funding of new technologies by public authorities, to ensure a high degree of synergy.

3.1.2 European Security Research Advisory Board (2005-2006) and the seventh research framework programme

3.1.2.1 The European Security Research Advisory Board

In 2005, the Commission established ESRAB ⁽²¹¹⁾. The group was composed of 50 experts in security appointed from users and industry and research organisations, divided into two groups addressing security research demand requirements and technology supply chain requirements, respectively. The Board's mission included outlining a strategic concept for the implementation of the security theme in FP7, providing clear implementation rules and drafting a communication strategy to promote awareness of European security research.

⁽²¹⁰⁾ European Commission, Commission communication, 'Security research: the next steps' (COM(2004) 590 final), Brussels, 7.9.2004.

⁽²¹¹⁾ Commission Decision of 22 April 2005 establishing the European Security Research Advisory Board (2005/516/EC), OJ L 191, 22.7.2005, p. 70-72.

ESRAB provided an initial definition of security research: ‘research activities that aim at identifying, preventing, deterring, preparing and protecting against unlawful or intentional malicious acts harming European societies; human beings, organisations or structures, material and immaterial goods and infrastructures, including mitigation and operational continuity after such an attack (also applicable after natural/industrial disasters)’ (European Commission, 2006).

Among the main tasks of ESRAB were to outline a comprehensive European security research agenda; to establish a network of users and technical experts to identify technological capabilities; to recommend a strategy to improve the European industry’s technological base; to advise on strategic and operational aspects of future security research and implementation rules; to optimise the use of publicly owned research and evaluation infrastructures; and to develop and implement a communication strategy to promote awareness of European security research. In September 2006, ESRAB published its final report *Meeting the Challenge: The European security research agenda* (European Commission, 2006), setting the priorities for security research under FP7 (Thoma, 2011).

ESRAB established a framework for structuring technology development, based on capabilities, and defined core and cross-cutting missions. The core missions were (i) border security, (ii) protection against terrorism and organised crime, (iii) critical infrastructure protection and (iv) restoring security in crisis situations. And the cross-cutting missions were (v) integration and interoperability, (vi) developing new capabilities and technologies and (vii) demonstration programmes.

ESRAB also recommended the creation of a European Security Board to ‘bring together, in a non-bureaucratic manner, authoritative senior representatives from a cross stakeholder community of public and private stakeholders to jointly develop a strategic security agenda and act as a possible reference body for the implementation of existing programmes and initiatives’ (European Commission, 2006) (see Section 3.1.3).

The ESRAB mandate concluded in December 2006.

3.1.2.2 The seventh research framework programme

FP7 was adopted in 2006 and covered the period 2007-2013. It had two main objectives: to strengthen the scientific and technological base of European industry, and to encourage international competitiveness while promoting research that supports EU policies.

FP7 was structured according to five specific programmes that constituted its major building blocks: cooperation, ideas, people, capacities and nuclear research. The cooperation programme represented two thirds of the overall budget and fostered collaborative research across Europe and other partner countries through projects.

The total budget for FP7 was more than EUR 50 billion. It included the first ESRP with a budget of EUR 1.4 billion, as one of the ten thematic areas ⁽²¹²⁾ within the cooperation programme. This represented the first fully fledged EU security research programme ⁽²¹³⁾.

The security theme under FP7 had an exclusively civil orientation, although the need for close coordination with the EDA on areas relating to dual-use technology was recognised ⁽²¹⁴⁾.

Space was a thematic area within FP7, with a budget similar to security.

Security research under FP7

The ESRP was conceived as a mission-driven programme, addressing four main security missions and three cross-cutting domains. Each mission was distributed into several sub-areas (**Figure 3**).

Six calls for proposals were published between 2007 and 2013. Of the 1 790 eligible proposals, 307 projects were funded through the FP7 security programme. The total cost of these projects was EUR 1 788 billion,

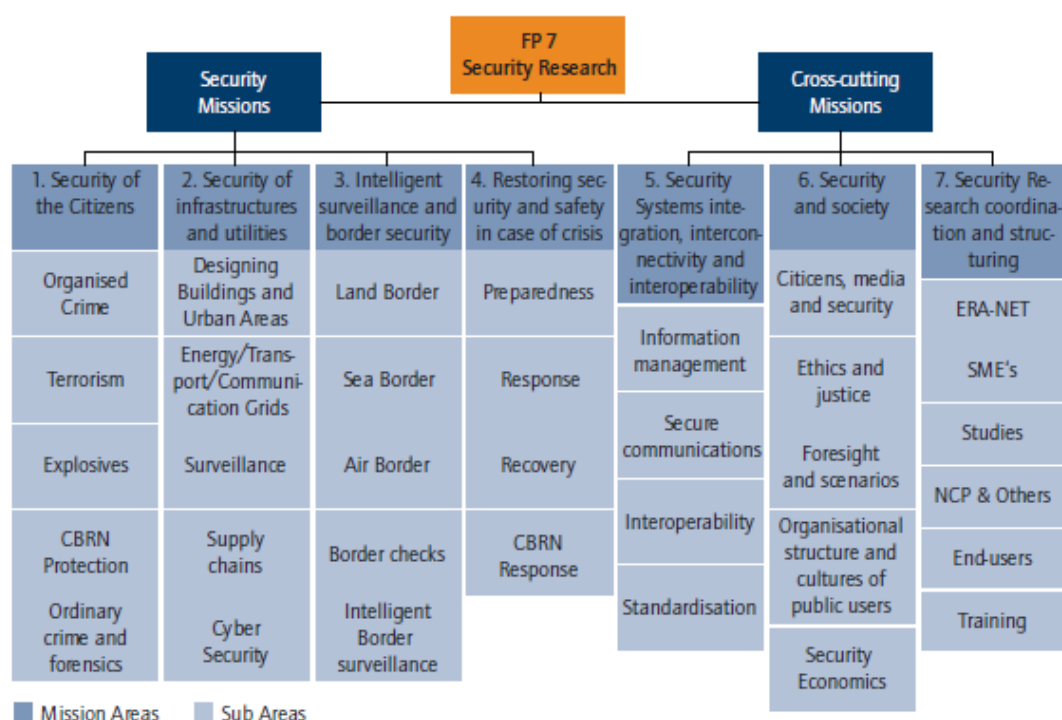
⁽²¹²⁾ Those were health; food, agriculture and fisheries, biotechnology; information and communication technologies; nanosciences, nanotechnologies, materials and new production technologies; energy; environment (including climate change); transport (including aeronautics); socioeconomic sciences and the humanities; space; and security

⁽²¹³⁾ DG Enterprise and Industry was originally responsible for the security research programme. On 1 January 2015, the Policy and Research and Security Unit moved from DG Enterprise and Industry to DG Migration and Home Affairs and became Unit B.4 of the DG, ‘Innovation and Industry for Security’. At the same time, DG Enterprise and Industry changed its name to DG Internal Market, Industry, Entrepreneurship and SMEs.

⁽²¹⁴⁾ Decision No 1982/2006/EC of the European Parliament and of the Council of 18 December 2006 concerning the seventh framework programme of the European Community for research, technological development and demonstration activities (2007-2013), Brussels, OJ L 412, 30.12.2006, p. 1-43.

with the Commission contributing EUR 1 263 billion (71 %) (European Commission, 2015). The distribution of projects and funding by mission is shown in **Table 3**.

Figure 3: Missions and cross-cutting areas of security research under FP7



Source: Thoma (2011).

Table 3: Distribution of projects, participation and funding in FP7 security research

Missions	Projects	Participations	Commission contribution
Security of citizens	18 %	18 %	19 %
Security of infrastructures and utilities	17 %	19 %	20 %
Intelligent surveillance and border security	10 %	12 %	17 %
Restoring security and safety in case of crisis	18 %	20 %	23 %
Security systems integration, interconnectivity and interoperability	10 %	8 %	8 %
Security and society	15 %	13 %	9 %
Security Research coordination and structuring	11 %	11 %	6 %
(Other)	1 %	0 %	0 %
Total	307	3.74	EUR 1.263 bn

Source: European Commission (2015).

3.1.3 The European Security Research and Innovation Forum

In September 2007, the Commission presented a communication on public-private dialogue in security research and innovation, which established the European Security Research and Innovation Forum (ESRIF) ⁽²¹⁵⁾. Its main objective was to develop a medium-to-long term strategy for EU security research with a specific agenda. Another aim was to share ideas, views and best practices to make better use of existing capabilities and to enhance the use of technology in security-related domains. It brought the 'innovation' part into the European agenda.

ESRIF was composed of policymakers, representatives of industry, of end-users of security research, and of academic and research institutions. It involved more than 600 experts and 65 personalities working in 11 specific working groups: security of citizens, security of critical infrastructures, border security, crisis management, foresight and scenarios, CBRN, situation awareness and the role of space, identification of people and assets, innovation issues, governance and coordination, and human and societal dynamics of security.

ESRIF's mandate ended in December 2009 with the publication of its final report (ESRIF, 2009) in which it proposed a European security research and innovation agenda (ESRIA) to run over the following 20 years, setting out the context, content and implementation of the agenda, and making recommendations to support the development of European security (see **Table 4**).

ESRIF made policy and operational recommendations for achieving stronger security research and innovation results. These were (i) draw on collective strengths and knowledge by developing common European capabilities, (ii) provide support for new policy initiatives, (iii) take an integrated approach to security, (iv) consider the global dimension of civil security and (v) consider ESRIA a living document that will evolve with threats across Europe.

Table 4: The ESRIA research content clusters and cluster components

ESRIA clusters	ESRIA cluster components
Cluster 1: Preventing, protecting, preparing, responding and recovering	Securing people
	Civil preparedness
	Crisis management
Cluster 2: Countering different means of attack	Explosives
	CBRN threats
	New technologies, new threats
Cluster 3: Securing critical assets	Security of critical infrastructures, security
	Security economics
Cluster 4: Securing identity, access and movement of people and goods	Border security
	Identity management and protection
Cluster 5: Cross-cutting enablers	Information and communication technology
	Space
	Evidence and forensics
	Informed decision making

Source: ESRIF (2009).

⁽²¹⁵⁾ European Commission, Commission communication, 'Public-private dialogue in security research and innovation' COM(2007) 511 final, Brussels, 11.9.2007.

In response to ESRI's work, the Commission presented a communication in December 2009, with its initial reactions to ESRI's key findings and recommendations⁽²¹⁶⁾. It also highlighted a number of topics for the following Commission to consider analysing further. Among these topics were the establishment of a permanent working structure to implement ESRI recommendations and the possibility of establishing a forum to strengthen the competitiveness of the security industry active in the field of research and innovation, such as a high-level group, with the involvement of all public sector, private sector and civil society stakeholders.

3.1.4 Other funding programmes related to security (2007-2013)

During the period 2007-2013, in addition to the FP7 security theme, there were a number of programmes and funds financing a wide variety of security related activities, which sometimes concerned research. They are briefly outlined hereafter.

3.1.4.1 The European Union framework programme on security and safeguarding liberties

The framework programme on security and safeguarding liberties⁽²¹⁷⁾ was composed of two specific programmes: the prevention of and fight against crime programme (ISEC)⁽²¹⁸⁾ and the prevention, preparedness and consequence management of terrorism and other security-related risks programme (CIPS)⁽²¹⁹⁾.

ISEC and CIPS covered a very broad policy field, which between 1993 and 2009 largely fell under the 'Police and judicial cooperation in criminal matters' pillar of the EU, as introduced by the Treaty of Maastricht.

ISEC replaced the framework programme on police and judicial cooperation in criminal matters⁽²²⁰⁾, which covered the period 2003-2006 and aimed to strengthen EU cross-border cooperation between police, other law enforcement agencies and judicial authorities. The total allocated budget for ISEC amounted to EUR 522 million for the whole period. The general objectives were to prevent and combat crime, particularly terrorism, trafficking of people, offences against children, drug trafficking, the arms trade and trafficking, cybercrime, corruption and fraud; and to contribute to the establishment of policies at EU level. The programme's four specific objectives addressed four main themes: (1) crime prevention and criminology, (2) law enforcement, (3) protection and support for witnesses and (4) protection of victims.

For its part, CIPS focused on critical infrastructure and other security issues, including operational aspects in areas such as crisis management and preparedness in various sectors of critical importance. Its total allocated budget amounted to EUR 126.8 million for the whole period. CIPS had two general objectives, prevention, and preparedness and consequence management, which were further divided into seven specific objectives⁽²²¹⁾. These covered several thematic areas: (i) crisis management, (ii) terrorism and other security-related risks within the area of freedom, security and justice, including risks relating to the environment, (iii) public health, (iv) transport, (v) R & T and (vi) economic and social cohesion.

Both programmes were implemented under the direct management of the Commission, and the main conclusions of their *ex post* evaluation were published in 2018⁽²²²⁾.

⁽²¹⁶⁾ European Commission, Commission communication, 'A European security research and innovation agenda — Commission's initial position on ESRI's key findings and recommendations' (COM (2009) 691 final), Brussels, 21.12.2009.

⁽²¹⁷⁾ European Commission, Commission communication, 'Establishing a framework programme on security and safeguarding liberties for the period 2007-2013' (COM(2005) 124 final), Brussels, 6.4.2005.

⁽²¹⁸⁾ Council Decision 2007/125/JHA, of 12 February 2007 establishing for the period 2007-2013, as part of the General Programme on Security and Safeguarding Liberties, the Specific Programme 'Prevention of and Fight against Crime', OJ L 58, 24.2.2007, p. 7-12.

⁽²¹⁹⁾ Council Decision 2007/124/EC, Euratom, of 12 February 2007 establishing for the period 2007 to 2013, as part of General Programme on Security and Safeguarding Liberties, the Specific Programme 'Prevention, Preparedness and Consequence Management of Terrorism and other Security-related risks', OJ L 58, 24.2.2007, p. 1-6.

⁽²²⁰⁾ Council Decision 2002/630/JHA of 22 July 2002 establishing a framework programme on police and judicial cooperation in criminal matters (AGIS), OJ L 203, 1.8.2002, p. 5-8.

⁽²²¹⁾ European Commission, Commission staff working document 'Ex-post evaluation of the "Prevention, Preparedness and Consequence Management of Terrorism and other Security related risks" 2007-2013 Programme (CIPS)' (SWD(2018) 331 final), accompanying Commission report COM(2018) 455 final, Brussels, 12.6.2018.

⁽²²²⁾ European Commission, Commission report, *Ex-post evaluation report for the period 2007-2013 of actions financed by the 'Prevention and fight against crime' programme (ISEC) and the 'Prevention, preparedness and consequence management of terrorism and other security related risks' programme (CIPS)* (COM(2018) 455 final), Brussels, 12.6.2018.

3.1.4.2 The External Borders Fund

The External Borders Fund (EBF)⁽²²³⁾ is the first EU instrument dedicated to funding external border management in the EU Member States, with a total budget of EUR 1.82 billion over the period 2007-2013. It was established as part of the more general programme 'Solidarity and management of migration flows', funded to EUR 4.0 billion, which also included the European Return Fund, the European Fund for Integration of Third-Country Nationals and the European Refugee Fund.

The EBF was set up to promote financial solidarity between Member States, by supporting those facing a heavy financial burden in implementing common standards on external border controls. It allocated its support according to five priorities⁽²²⁴⁾: (1) setting up of a common integrated border management system in respect of checks on persons and the surveillance of the external borders, (2) developing and implementing the national components of a European surveillance system for the EU's external borders and of a permanent European patrol network for the southern maritime borders, (3) issuing visas and tackling illegal immigration, (4) establishing the IT systems required to implement EU border and visa legislation and (5) promoting the effective and efficient application of EU border and visa legislation.

The EBF was implemented under shared management arrangements with national programmes. It also funded community actions and specific actions, which were directly managed by the European Commission and implemented by Member States.

The European Court of Auditors provided recommendations on the implementation of this fund, which were taken into account by the Commission for the following period (European Court of Auditors, 2014). The successor of the EBF for 2014-2020 was the Instrument for Financial Support for External Borders and Visa, as part of the ISF.

3.1.4.3 The competitiveness and innovation framework programme

The competitiveness and innovation framework programme (CIP)⁽²²⁵⁾ aimed to encourage the competitiveness of European enterprises. With SMEs as its main target, it supported innovation activities (including eco-innovation), provided better access to finance and delivered business support services in the regions. It encouraged better take-up and greater use of ICT and helped to develop the information society. It also promoted increased use of renewable energies and energy efficiency.

The CIP ran from 2007 to 2013 and was organised around three multiannual programmes, each with specific objectives⁽²²⁶⁾: (1) the entrepreneurship and innovation programme, (2) the information communication technologies policy support programme and (3) the intelligent energy Europe programme.

The overall budget was EUR 3 621 million, distributed approximately as follows: EUR 2 166 million for the entrepreneurship and innovation programme (60 %), EUR 728 million for the information communication technologies policy support programme and EUR 727 million for the intelligent energy Europe programme.

The information communication technologies policy support programme aimed to achieve wider uptake and greater use of ICT by citizens, governments and businesses, in particular SMEs. It mainly supported pilot projects and experience sharing in areas such as health, ageing and inclusion, digital libraries, government and governance, energy efficiency, the environment and smart mobility, public sector information, and internet evolution and security.

The evaluation of the CIP was carried out in 2011 (Centre for Strategy and Evaluation Services, 2011b), with a summary of its overall performance presented by the joint CIP committees in 2013 (European Commission, 2013a). The Commission highlighted the findings and recommendations of the overall evaluations in its report *Evaluations of the Competitiveness and Innovation Framework Programme*⁽²²⁷⁾. It made some

⁽²²³⁾ Decision No 574/2007/EC of the European Parliament and of the Council of 23 May 2007 establishing the External Borders Fund for the period 2007 to 2013 as part of the general programme 'Solidarity and management of migration flows', OJ L 144, 6.6.2007, p. 22-44.

⁽²²⁴⁾ Commission Decision of 27 August 2007 implementing Decision No 574/2007/EC of the European Parliament and of the Council as regards the adoption of strategic guidelines for 2007 to 2013 (2007/599/EC), OJ L 233, 5.9.2007, p. 3-6.

⁽²²⁵⁾ Decision No 1639/2006/EC of the European Parliament and of the Council of 24 October 2006 establishing a competitiveness and innovation framework programme (2007 to 2013), OJ L 310, 9.11.2006, p. 15-40.

⁽²²⁶⁾ CIP, 'What Is CIP?' (http://ec.europa.eu/cip/files/docs/factsheets_en.pdf).

⁽²²⁷⁾ European Commission, Commission report, *Evaluations of the Competitiveness and Innovation Framework Programme* (COM(2013) 2 final), Brussels, 15.1.2013.

recommendations in particular on how to further improve the implementation of the CIP and design a possible successor programme.

For the period 2014-2020, the successor of CIP is the programme for the competitiveness of enterprises and SMEs (COSME) and parts of H2020.

3.1.5 Horizon 2020 (2014-2020)

Horizon 2020 is the (8th) European framework programme for research and innovation ⁽²²⁸⁾, covering the period 2014-2020. It supports research and innovation projects and programmes in groundbreaking basic research, strategic and applied research, demonstration projects and close-to-market activities. It is the financial instrument implementing the Innovation Union, a Europe 2020 flagship initiative aimed at securing Europe's global competitiveness. In principle, H2020 combines all research and innovation funding previously provided through the framework programmes for R & T and the innovation-related activities of the CIP and the EIT. Its total budget is EUR 70.2 billion for the period 2014-2020, with prices fixed at 2011 levels.

H2020 consists of three main research areas or priorities (**Figure 4**):

1. excellent science, which focuses on basic science;
2. industrial leadership, with the goal of finding ways to modernise European industries that have suffered from a fragmented European market, based on the Europe 2020 and Innovation Union strategies;
3. societal challenges, which funds potential solutions to social and economic problems with a focus on implementing solutions, rather than technology development.

The framework programme is implemented by the European Commission. Its objective is to complete the European Research Area by coordinating national research policies and pooling research funding in certain areas to avoid duplication. H2020 itself is seen as a policy instrument for implementing other high-level policy initiatives of the EU, such as Europe 2020 and Innovation Union (i.e. the priority 'Societal challenges' responds directly to the policy priorities and societal challenges that are identified in the Europe 2020 strategy).

Figure 4: Structure of Horizon 2020

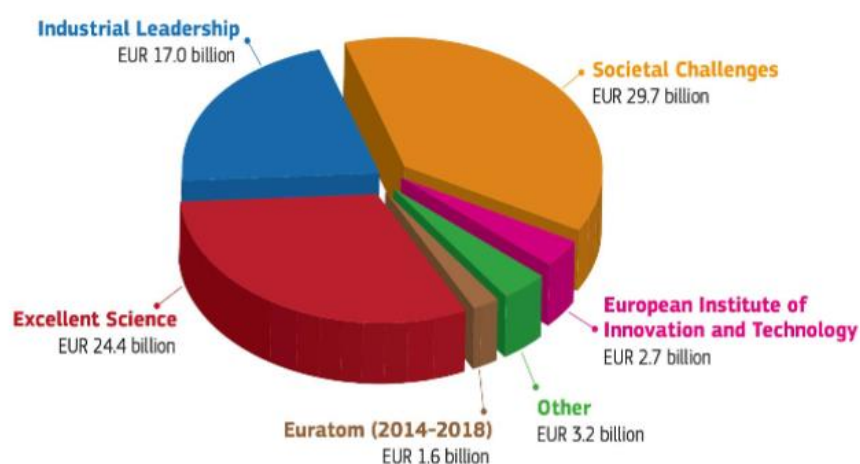
Excellent science	Industrial Leadership	Societal challenges
The European Research Council	Leadership in enabling and industrial technologies (space, ICT, etc.)	Health, demographic change and well-being
Future and Emerging Technologies	Access to risk finance	European Bioeconomy Challenges
Marie Skłodowska-Curie Actions	Innovation in SMEs	Secure, clean and efficient energy
European research infrastructures		Smart, green and integrated transport
		Climate action, resource efficiency (including raw materials)
		Europe in a changing world – Inclusive, innovative and reflective societies
		Secure societies

Source: Regulation (EU) No 1291/2013.

⁽²²⁸⁾ Regulation (EU) No 1291/2013 of the European Parliament and of the Council of 11 December 2013 establishing Horizon 2020 — the Framework Programme for Research and Innovation (2014-2020) and repealing Decision No 1982/2006/EC, Strasbourg, OJ L 347, 20.12.2013, p. 104-173; see also European Commission, 'What is Horizon 2020?' (<https://ec.europa.eu/programmes/horizon2020/what-horizon-2020>).

Figure 5 represents the distribution of the H2020 budget by priority.

Figure 5: Distribution of H2020 budget



Source: European Commission (2013b).

For the priority ‘Societal challenges’, the total budget of EUR 29.7 billion is further distributed among seven areas, as shown in **Table 5**; societal challenge 7 — ‘Secure societies’ — accounts for a little less than 6 % of the budget.

Table 5: Distribution of budget for Societal challenges under H2020 ⁽³⁶⁾

Total funding for 2014-2020	(million EUR)
<i>Priority 3: Societal challenges</i>	29 679
1. Health, demographic change and wellbeing	7 472
2. Food security, sustainable agriculture, etc.	3 851
3. Secure, clean and efficient energy	5 931
4. Smart, green and integrated transport	6 339
5. Climate action, resource efficiency, raw materials	3 081
6. Inclusive societies	1 309
7. Secure societies	1 695

Source: European Commission (2013b).

3.1.5.1 Secure Societies Challenge

Security research under H2020 is funded through the Secure Societies Challenge. This challenge is about undertaking the research and innovation activities needed to protect EU citizens, society and the economy as well as infrastructures and services, to ensure the EU's prosperity, political stability and well-being.

The key objectives of the Secure Societies Challenge ⁽²²⁹⁾ can be summarised as follows:

- border security and external security — to improve border security, ranging from improved maritime border protection to supply chain security, and to support the EU's external security policies, including through conflict prevention and peace building;
- fighting against crime and terrorism — it requires new technologies and capabilities for fighting and preventing crime (including cybercrime), illegal trafficking and terrorism (including cyberterrorism), including understanding and tackling terrorist ideas and beliefs to also avoid aviation-related threats;
- disaster-resilience — to enhance the resilience of our society against natural and man-made disasters, ranging from the development of new crisis management tools to increasing communication interoperability, and to develop novel solutions for the protection of critical infrastructure;
- digital security — to provide enhanced cybersecurity, ranging from secure information sharing to new assurance models, to ensure privacy and trust.

The Secure Societies Challenge contributes to the implementation of the policy goals of the Europe 2020 strategy, the security industrial policy, the internal security strategy and the cybersecurity strategy.

Detailed topics relating to these objectives are to be found in three H2020 Secure Societies work programmes (2014-2015, 2016-2017 and 2018-2020) ⁽²³⁰⁾, the objectives of which are summarised in **Table 6**.

The current H2020 work programme focuses its efforts on fewer topics with bigger budgets, directly supporting the Commission's political priorities. Four focus areas receive a combined budget of over EUR 7 billion: (1) building a low-carbon, climate resilient future, (2) connecting economic and environmental gains — the circular economy, (3) digitising and transforming European industry and services, and (4) boosting the effectiveness of the security union.

The focus area 'Boosting the effectiveness of the security union' (European Commission, 2017c), with a budget of EUR 1.074 billion, supports the implementation of the security union priorities and helps in tackling the challenges that Europe is facing on multiple fronts, such as cybercrime and other crimes, security threats and threats to infrastructure, natural and man-made disasters, and hybrid threats. Research on these threats, notably from terrorism, will underpin an effective and coordinated EU response, and better tools will reduce loss of life and material damage.

Table 6: Evolution of topics in the Horizon 2020 Secure Societies work programmes (WPs)

WP 2014-2015		WP 2016-2017	WP 2018-2020
Disaster - resilience	Crisis management	Critical infrastructure protection	Protecting infrastructure and people in the European smart cities
	Disaster resilience and climate change		
	Critical infrastructure protection		

⁽²²⁹⁾ Council Decision 2013/743/EU of 3 December 2013 establishing the specific programme implementing Horizon 2020 — the Framework Programme for Research and Innovation (2014-2020) and repealing Decisions 2006/971/EC, 2006/972/EC, 2006/973/EC, 2006/974/EC and 2006/975/EC, OJ L 347, 20.12.2013, p. 965-1041.

⁽²³⁰⁾ European Commission, 'Secure societies — protecting freedom and security of Europe and its citizens' (<https://ec.europa.eu/programmes/horizon2020/en/h2020-section/secure-societies-%E2%80%93-protecting-freedom-and-security-europe-and-its-citizens>).

WP 2014-2015		WP 2016-2017		WP 2018-2020	
	Communication technologies and interoperability				
	Ethical/ societal dimension				
Fight against crime and terrorism	Forensics	Security	Disaster -resilience: safeguarding and securing society	Security	Disaster-resilient societies
	Law enforcement capabilities		Fight against crime and terrorism		Fight against crime and terrorism
	Urban security		Border security and external security		Border and external security
	Ethical/ societal dimension		General matters		General matters
Digital security: cybersecurity, privacy and trust		Digital security		Digital security	Cybersecurity, digital privacy and data protection
					Management of cyber-attacks and other risks
Border security and external security	Maritime border security				
	Border crossing points				
	Supply chain security				
	External security				
	Ethical/ societal dimension				

Source: European Commission, 'Secure societies — protecting freedom and security of Europe and its citizens' (<https://ec.europa.eu/programmes/horizon2020/en/h2020-section/secure-societies-%E2%80%93-protecting-freedom-and-security-europe-and-its-citizens>).

3.1.6 Other funds related to security (2014-2020)

In addition to H2020, there were a number of programmes and funds financing a wide variety of security-related activities, which sometimes concerned research. These are briefly outlined hereafter.

3.1.6.1 The Internal Security Fund

The ISF was set up for the period 2014-2020, with a total budget of EUR 3.8 billion. The ISF promotes the implementation of the internal security strategy, law enforcement cooperation and the management of the EU's external borders. It is composed of two instruments: ISF Borders and Visa, and ISF Police.

ISF Borders and Visa ⁽²³¹⁾

This instrument's main objective is to contribute to ensuring a high level of security in the EU while facilitating legitimate travel. This goal is achieved by supporting actions with the following specific objectives:

- visa — to process effectively Schengen visas by supporting a common visa policy, providing a high quality of service to visa applicants, ensuring equal treatment of non-EU nationals and tackling irregular migration;
- borders: to achieve a high level of control of the external borders by supporting integrated border management, harmonising border management measures within the EU and sharing information among EU Member States and with Frontex, to halt irregular migration and enable smooth crossing of the external borders

A total budget of EUR 2.76 billion is available for funding actions under the ISF Borders and Visa instrument, of which EUR 1.55 billion is channelled through shared management and EUR 1.06 billion through direct management.

Specific actions funded through this instrument include setting up and running IT systems, acquisition of operational equipment, promoting and developing training schemes, and ensuring administrative and operational coordination and cooperation.

ISF Police ⁽²³²⁾

This instrument focuses on two objectives:

1. Fight against crime: combating cross-border, serious and organised crime including terrorism, and fight against crime — combating cross-border, serious and organised crime including terrorism, and reinforcing cooperation between EU Member State law enforcement authorities, relevant EU bodies, such as Europol, and non-EU and international organisations;
2. Managing risk and crisis — enhancing the EU's capacity to manage effectively security-related risk and crisis, and protect people and critical infrastructures against terrorist attacks and other security incidents.

A total budget of slightly over EUR 1 billion is available for funding actions under the ISF Police instrument, of which EUR 662 million is channelled through shared management and EUR 342 million through direct management.

The specific actions funded through this instrument include initiatives similar to those mentioned above in relation to ISF Borders and Visa.

⁽²³¹⁾ European Parliament and Council of the European Union Regulation (EU) No 515/2014.

⁽²³²⁾ European Parliament and Council of the European Union Regulation (EU) No 513/2014.

3.1.6.2 The Asylum, Migration and Integration Fund

AMIF⁽²³³⁾ was set up for the period 2014-2020, with a total of EUR 3.137 billion. It supports national and EU initiatives that promote the efficient management of migration flows and the implementation, strengthening and development of a common EU approach to asylum and immigration. This fund contributes to the achievement of four specific objectives:

- asylum — strengthening and developing the Common European Asylum System by ensuring that EU legislation in this field is efficiently and uniformly applied;
- legal migration and integration — supporting legal migration to EU Member States in line with labour market needs and promoting the effective integration of non-EU nationals;
- return — creating fair and effective return strategies that contribute to combating irregular migration, with an emphasis on the sustainability and effectiveness of the return process;
- solidarity — making sure that the EU Member States that are most affected by migration and asylum flows can count on solidarity from other EU Member States.

This fund also provides financial resources for other activities, such as the European Migration Network, the Union Resettlement Programme and the transfer of beneficiaries of international protection from an EU Member State with high migratory pressure to another.

Most AMIF funds⁽²³⁴⁾ (approximately 88 %) are channelled through shared management. The rest is divided between EU actions and emergency assistance, to be implemented through direct management.

3.1.6.3 The programme for the competitiveness of enterprises and small and medium-sized enterprises

The goal of the programme COSME⁽²³⁵⁾ is to contribute to the creation of jobs and economic growth by strengthening the competitiveness and sustainability of EU enterprises, particularly SMEs; encouraging entrepreneurial culture; and promoting the creation and growth of SMEs. Its planned budget amounts to EUR 2.3 billion.

COSME has four specific objectives: (1) to improve access to finance for SMEs in the form of equity and debt, (2) to improve access to markets, (3) to improve framework conditions for the competitiveness and sustainability of EU enterprises and (4) to promote entrepreneurship and entrepreneurial culture.

The Executive Agency for Small and Medium-sized Enterprises oversees the implementation of the COSME programme on behalf of the European Commission⁽²³⁶⁾.

An example of activities under this programme is in the COSME Call 2017, in the cluster 'Go international' in the defence and security sector. The main objective of the activities under 'Go international' was to support European defence- and security-related clusters and business network organisations to intensify collaboration across borders with other non-defence industrial clusters and to develop and implement joint strategies with non-EU countries in relation to dual-use technologies, products and services.

3.1.6.4 The justice programme

The justice programme⁽²³⁷⁾ offers financial support to various organisations specialising in the area of justice. The general objective is to contribute to the further development of a European area of justice based on mutual recognition and mutual trust, in particular by promoting judicial cooperation on civil and criminal matters. A budget of EUR 378 million has been allocated to achieve this.

⁽²³³⁾ Regulation (EU) No 516/2014 of the European Parliament and of the Council of 16 April 2014 establishing the Asylum, Migration and Integration Fund, amending Council Decision 2008/381/EC and repealing Decisions No 573/2007/EC and No 575/2007/EC of the European Parliament and of the Council and Council Decision 2007/435/EC, OJ L 150, 20.5.2014, p. 168-194.

⁽²³⁴⁾ Specific actions funded through AMIF include improvement of services for asylum seekers, campaigns on legal migration in non-EU countries, training for non-EU nationals, etc.

⁽²³⁵⁾ Regulation (EU) No 1287/2013 of the European Parliament and of the Council of 11 December 2013 establishing a programme for the competitiveness of enterprises and small and medium-sized enterprises (COSME) (2014-2020) and repealing Decision No 1639/2006/EC, OJ L 347, 20.12.2013, p. 33-49.

⁽²³⁶⁾ With the exception of the financial instruments delegated to the European Investment Fund.

⁽²³⁷⁾ Regulation (EU) No 1382/2013 of the European Parliament and of the Council of 17 December 2013 establishing a Justice Programme for the period 2014 to 2020, Brussels, OJ L 354, 28.12.2013, p. 73-83.

The programme focuses on the following key areas: (i) judicial cooperation on civil matters, including civil and commercial matters, insolvencies, family matters and succession, etc., (ii) judicial cooperation on criminal matters, (iii) judicial training, including linguistic training on legal terminology, with a view to fostering a common legal and judicial culture, (iv) enabling effective access to justice in Europe, including protecting the rights of victims of crime and procedural rights in criminal proceedings and (v) initiatives in the field of drugs policy (judicial cooperation and crime prevention aspects).

3.1.6.5 The rights, equality and citizenship programme

The rights, equality and citizenship programme 2014-2020 ⁽²³⁸⁾ defends the rights and freedoms that people are entitled to under EU law. Its total budget is EUR 439.5 million.

The specific objectives of the programme are (i) to promote non-discrimination, (ii) to combat racism, xenophobia, homophobia and other forms of intolerance, (iii) to promote gender equality and gender mainstreaming, (iv) to prevent violence against children, young people, women and other groups at risk, (v) to promote the rights of the child, (vi) to ensure the protection of personal data in the EU, (vii) to promote EU citizenship rights and (viii) to enforce consumer rights.

3.1.7 Security advisory groups after the European Security Research and Innovation Forum

3.1.7.1 Security advisory groups for the seventh framework programme (2007-2013)

The Security Advisory Group (2007-2009)

The Security Advisory Group was created in 2007, by the European Commission, as one of the 16 advisory groups set up for the various themes of FP7, with the purpose of advising the Commission on the implementation of the research programme. It started with 20 members, some of them already having participated in ESRI. The Security Advisory Group and ESRI coexisted during the period 2007-2009.

Members of the group provided advice to the Commission services on strategy, relevant objectives, and scientific and technological priorities, regarding the security theme of the cooperation specific programme. Input was provided in written form ⁽²³⁹⁾ to support the preparation of the annual work programme.

The Security Advisory Group (2009-2013)

The Security Advisory Group was revised in 2009, being constituted of 21 individual experts from security end-user organisations, academia and industry, plus 3 members from the Commission. The membership changed every 2 years. The group produced two reports, in 2011 and 2012 ⁽²⁴⁰⁾.

3.1.7.2 Security advisory groups for Horizon 2020 (2014-ongoing)

Secure Societies Advisory Group (2014-2016)

Under the specific programme implementing Horizon 2020 (2014-2020), the Commission continued to be assisted by expert groups in drawing up the multiannual work programmes. A registry of expert groups is publicly available, where the participants are identified and their activities published ⁽²⁴¹⁾.

In January 2014, the Secure Societies Advisory Group was established to provide advice regarding the Secure Societies Challenge. It provided in particular strategic input for the 2016-2017 call of the Secure Societies Challenge in July 2014, and in December 2015 it presented strategic recommendations to the European Commission on how the 'Secure societies' theme in H2020 should be developed to address longer-term priorities and opportunities ⁽²⁴²⁾.

⁽²³⁸⁾ Regulation (EU) No 1381/2013 of the European Parliament and of the Council of 17 December 2013 establishing a Rights, Equality and Citizenship Programme for the period 2014 to 2020, OJ L 354, 28.12.2013, p. 62-72.

⁽²³⁹⁾ For Security Advisory Group reports, see European Commission, 'Advisory groups for FP7 — documents for the first two years of FP7 implementation' (https://ec.europa.eu/research/fp7/index_en.cfm?pg=eag-1st2years).

⁽²⁴⁰⁾ For mandate and reports, see European Commission, 'Advisory groups for FP7' (http://ec.europa.eu/research/fp7/index_en.cfm?pg=eag).

⁽²⁴¹⁾ European Commission, 'Register of Commission expert groups and other similar entities' (<http://ec.europa.eu/transparency/regexpert/>; Consulted on 12 February 2019).

⁽²⁴²⁾ For mandate and reports, see European Commission, 'Group details — Commission expert group' (<http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetail&groupID=3010>).

Horizon 2020 Protection and Security Advisory Group (2016-2018)

In 2016, the group was renewed and renamed the Horizon 2020 Protection and Security Advisory Group. In July 2017, it produced recommendations on international cooperation on security research, and in December 2017 a document on developing capabilities and enhancing various subsectors of the industry ⁽²⁴³⁾

Horizon 2020 Protection and Security Advisory Group (PASAG) (2018-2020)

A new mandate has been introduced for the period 2018-2020; it will end on 31 December 2020, at the same time as H2020. This group has not yet produced any specific input, although its activities and meeting minutes can be found in the registry of expert groups ⁽²⁴⁴⁾.

3.1.8 Horizon Europe (2021-2027)

In June 2018, the Commission published a proposal for a regulation establishing Horizon Europe, the new framework programme for research and innovation that will succeed H2020, from 2021 to 2027 ⁽²⁴⁵⁾.

Horizon Europe's general objective is to deliver scientific, economic and societal impact from the EU's investments in research and innovation, in order to strengthen its scientific and technological base and foster its competitiveness — including that of its industry — deliver on its strategic priorities and contribute to tackling global challenges, including the Sustainable Development Goals.

The programme has the following specific objectives:

- to support the creation and diffusion of high-quality new knowledge, skills, technologies and solutions to global challenges;
- to strengthen the impact of research and innovation in developing, supporting and implementing EU policies, and support the uptake of innovative solutions in industry and society to address global challenges;
- to foster all forms of innovation, including breakthrough innovation, and strengthen market deployment of innovative solutions;
- to optimise delivery for increased impact within a strengthened European Research Area.

The Horizon Europe programme will be implemented through three pillars (**Figure 6**):

1. The 'Open science' pillar (EUR 25.8 billion) supports frontier research projects chosen and driven by researchers themselves through the European Research Council (EUR 16.6 billion), funds fellowships and exchanges for researchers through Marie Skłodowska-Curie actions (EUR 6.8 billion) and invests in world-class research infrastructures.
2. The 'Global challenges and industrial competitiveness' pillar (EUR 52.7 billion) directly supports research relating to societal challenges, reinforces technological and industrial capacities and establishes EU-wide missions with ambitious goals to tackle some of our biggest problems. It also includes activities pursued by the JRC (EUR 2.2 billion).
3. The 'Open innovation' pillar (EUR 13.5 billion) aims to make Europe a frontrunner in market-creating innovation through the European Innovation Council (EUR 10 billion). It will help to develop the overall European innovation landscape, including by further strengthening the EIT to foster the integration of business, research, higher education and entrepreneurship (EUR 3 billion).

⁽²⁴³⁾ For mandate and reports, see European Commission, 'Group details — Commission expert group' (<http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetail&groupId=3010>).

⁽²⁴⁴⁾ For mandate and reports, see European Commission, 'Group details — Commission expert group' (<http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetail&groupId=3010>).

⁽²⁴⁵⁾ European Commission, 'Proposal for a Regulation of the European Parliament and of the Council establishing Horizon Europe — the Framework Programme for Research and Innovation, laying down its rules for participation and dissemination' (COM(2018) 435 final), Brussels, 7.6.2018.

Figure 6: Proposed structure of Horizon Europe



Source: European Commission proposal COM(2018) 435 final.

The proposed budget allocation of EUR 100 billion for the 7 years includes EUR 97.6 billion under Horizon Europe (EUR 3.5 billion of which will be allocated through the InvestEU Fund) and EUR 2.4 billion for the Euratom research and training programme.

Horizon Europe and the Euratom research and training programme will promote effective and operational synergies with other future EU programmes and policies to promote faster dissemination and uptake of research and innovation results, including the EU cohesion policy (which plays an important part in EU funding for research and innovation through an increased focus on innovation and smart specialisation strategies), the new EDF (EUR 13 billion, EUR 4.1 billion of which will be devoted to defence research), the international fusion energy project ITER (EUR 6.1 billion), the digital Europe programme (EUR 9.2 billion for investments in high-performance computing and data, AI, cybersecurity and advanced digital skills), and the Connecting Europe Facility (EUR 3 billion to support the digital single market).

3.1.8.1 'Inclusive and secure society' (Cluster 2)

In the current proposal for Horizon Europe, the security theme is one of the five clusters that compose the second pillar 'Global challenges and industrial competitiveness'. The cluster is named 'Inclusive and secure society' and the proposed budget is EUR 2.8 billion. As the cluster includes the topic of inclusive societies, it is estimated that the budget dedicated to security as such will be similar to that allocated in H2020.

The objectives of the cluster are the following, with the last two related to security:

- strengthen European democratic values and address issues of trust;
- safeguard and promote our cultural heritage;
- take advantage of socioeconomic transformations and promote inclusive growth while responding to globalisation and technological advancements;
- prepare for and respond to human-made and natural disasters, such as climate-related extreme weather events, terrorism, earthquakes;
- respond to changing security threats, both physical and digital, and support EU border management.

The cluster covers the following six intervention areas, with the last three referring to security ⁽²⁴⁶⁾: (1) democracy, (2) cultural heritage, (3) social and economic transformations, (4) disaster-resilient societies, (5) protection and security, and (6) cybersecurity.

⁽²⁴⁶⁾ There is continuity in the areas of intervention in security research between H2020 and Horizon Europe: (i) 'Disaster-resilient societies' corresponds to the area of the same name in 'Secure societies — Societal Challenge 7' (SC7); (ii) 'Protection and security' is related to the SC7 areas 'Infrastructure protection', 'Fight against crime and terrorism' and 'Border and external security'; and (iii) 'Cybersecurity' corresponds to the area 'Digital security' in SC7.

In more detail, the topics covered by some of the areas of intervention related to the security theme are the following.

— Disaster-resilient societies:

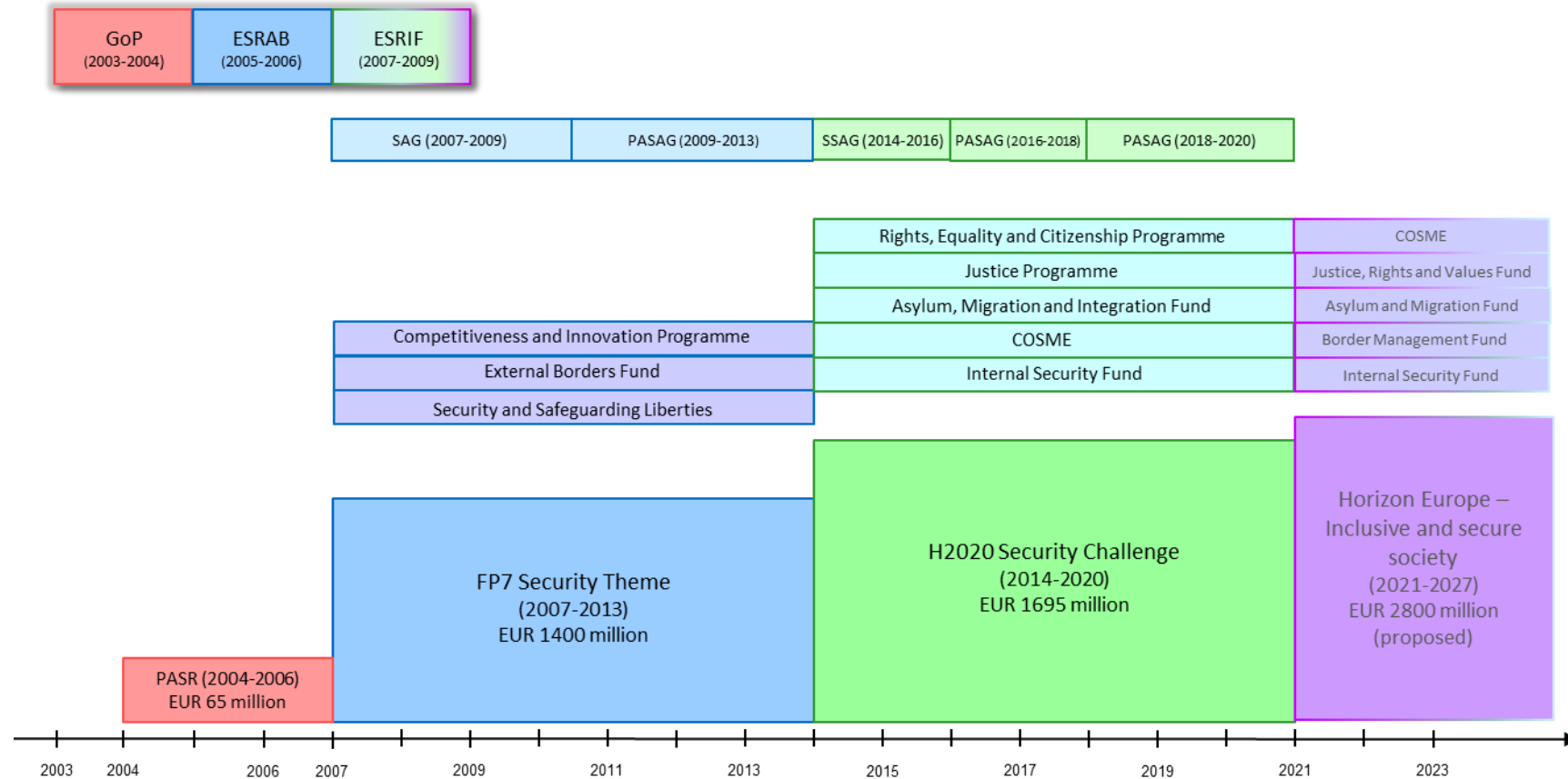
- technologies and capabilities for first responders for emergency operations in crisis and disaster situations;
- the capacity of society to better manage and reduce disaster risk, including through nature-based solutions, by enhancing prevention, preparedness and response to existing and new risks;
- interoperability of equipment and procedures to facilitate cross-border operational cooperation and an integrated EU market.

— Protection and security:

- innovative approaches and technologies for security practitioners (e.g. police forces, border and coast guards, customs offices), public health practitioners, operators of infrastructure and those managing open spaces;
- human and social dimensions of criminality and violent radicalisation, in relation to those engaged or potentially engaged in such behaviour as well as to those affected or potentially affected;
- addressing the mindset of citizens, public authorities and industry to prevent the creation of new security risks and to reduce existing risks, including those from new technologies such as AI;
- combating disinformation and fake news with implications for security;
- interoperability of equipment and procedures to facilitate cross-border and interagency operational cooperation and develop an integrated EU market.
- ensuring the protection of personal data in law enforcement activities, in particular in view of rapid technological developments.

An overview of the chronological evolution of the European security research structure, including advisory bodies, is provided in **Figure 7**, going from the first steps in the early 21st century to the soon-to-start Horizon Europe framework programme.

Figure 7: Overview of European security research, including advisory bodies



Note: GoP: Group of Personalities; ESRAB: European Security Research Advisory Board; ESRIF: European Security Research and Innovation Forum; SAG: Security Advisory Group; SSAG: Secure Societies Advisory Group; PASAG: Protection and Security Advisory Group

Source: Authors

3.2 History and evolution of European Union defence research

Graphical overview of the evolution of the European Defence Research under EU funds and associated legislation with a timeline is presented in **Figure 10**.

3.2.1 European Defence Agency — first research activities outside the European Union budget

In 2004, the European Council created to complement the European security strategy the EDA, an intergovernmental agency to be active in the field of developing defence capabilities, research, acquisitions and armaments. In pursuing its mission to develop capabilities in support of the CSDP, the EDA carries out R & T activities. In December 2005, the EDA awarded the first defence R & T contract. More than EUR 500 million has been allocated to over 150 R & T projects by Member States since the EDA's creation. However, the EDA's research activities have been funded not from the EU budget but by the participant countries.

R & T activities are managed through the EDA capability technology groups, or CapTechs, which form a network of experts from participating Member States dedicated to a particular technology area. The strategic research agendas are important tools that provide strategic guidance on the R & T priorities addressed in the various CapTechs. There are 12 CapTechs, 6 on military capabilities (communication and information systems, simulation, aerial systems, ground systems, naval systems and ammunition technologies) and 6 on cross-cutting enablers (materials and structures, technologies for components and modules, radiofrequency sensor technologies, electro-optical sensor technologies, CBRN and human factors, and guidance, navigation and control), plus 2 working groups ⁽²⁴⁷⁾.

3.2.2 The Commission communication of July 2013

In 2007, the European Commission presented a communication ⁽²⁴⁸⁾ highlighting the importance of improving the long-term competitiveness of the defence industry for Europe's security and defence ambitions. It also included a number of policy measures to strengthen the defence industry market, including the pooling of R & D investment. According to a European Parliament report of 2016, *The Future of EU Defence Research* (European Parliament, 2016a), this communication was the first ever European political document to emphasise the importance of defence research.

In July 2013, the European Commission presented a communication ⁽²⁴⁹⁾ calling for the exploitation of the dual-use potential synergies between civil and military research, such as civil applications developed under the H2020 'Secure societies' theme (including KETs), and mentioning the coordination between the FP7 security theme and European defence research activities. In addition, one of the actions set out in the communication reads: 'The Commission will consider the possibility to support CSDP-related research, such as through a Preparatory Action. The focus would be on those areas where EU defence capabilities would be most needed, seeking synergies with national research programmes where possible.' This was the first call for specific action on defence research.

This communication was supported by the European Parliament and the Council of the European Union ⁽²⁵⁰⁾. Then the European Council of December 2013 ⁽²⁵¹⁾ decided to review progress in June 2015 and invited the Member States to increase their investment in cooperative research programmes, informing them that a preparatory action on CSDP-related research would be set up.

A year later, the Commission presented an implementation roadmap for the communication 'A new deal for European defence' ⁽²⁵²⁾. One of its points was dedicated entirely to 'Exploiting dual-use potential of research and reinforcing innovation', establishing two deliverables:

⁽²⁴⁷⁾ More information can be found at the EDA website (<https://eda.europa.eu>).

⁽²⁴⁸⁾ European Commission, Commission communication, 'A strategy for a stronger and more competitive European defence industry' (COM(2007) 764 final), Brussels, 5.12.2007.

⁽²⁴⁹⁾ European Commission communication, 'Towards a more competitive and efficient defence sector' (COM(2013) 542 final), Brussels, 24.7.2013.

⁽²⁵⁰⁾ European Parliament Resolution 2013/2105(INI) on the implementation of the common security and defence policy (based on the annual report from the Council to the European Parliament on the common foreign and security policy), Strasbourg, 21 November 2013; Council of the European Union conclusions 15992/13.

⁽²⁵¹⁾ Council of the European Union conclusions EUCO 217/13.

⁽²⁵²⁾ European Commission report COM(2014) 387 final.

1. **Dual-use research.** This deliverable included the maximisation of synergies between the civil research under H2020 and the defence research coordinated by the EDA, and the identification of innovation fields and applications (including KETs and civil sectors of high interest to the defence and security industries);
2. **Preparatory action.** This was intended to illustrate the added value of an EU contribution to new research areas, complementing the CSDP-related civilian research ongoing under H2020. The preparatory action is covered in Section 3.2.6.

3.2.3 The European defence action plan (2016)

In November 2016, the Commission took a further step towards the development of EU defence research and presented the European defence action plan⁽²⁵³⁾, which included the establishment of the EDF and other actions to support Member States in more efficient spending on joint defence. The plan followed up on the Commission communication of July 2013 and on the conclusions of the European Council of December 2013, and it had three pillars: (1) the launch of the EDF, (2) the defence supply chain and (3) the single market for defence.

Further details on the EDF were published by the European Commission in June 2017 (see Section 3.2.7).

Also in June 2017, the Commission published a reflection paper⁽²⁵⁴⁾ presenting three different scenarios for future cooperation on the defence area in the EU, moving from cooperation to shared security and on to common defence and security.

3.2.4 First steps in European Union-funded defence research: the pilot project (2015-2016)

The first fully fledged security research programme, which started under FP7 (the security theme), and the subsequent programme under H2020 ('Secure societies') had an exclusively civil orientation, although the need for close coordination with the EDA on areas relating to dual-use technology was recognised (see Section 3.1). So far, defence research had not been covered under the research framework programmes.

In 2014, the European Parliament proposed an amendment to the EU budget to introduce a pilot project on defence research. The aim was to test and assess certain governance aspects in relation to the PADR and the capacity of the EDA to act as an executive agency to implement research on security and defence (European Parliament, 2016b). The pilot project was entrusted to the EDA⁽²⁵⁵⁾ by the European Commission through a delegation agreement giving it responsibility for the execution and management of the projects.

The pilot project was launched in 2015 and ran from 1 December 2015 until 1 December 2018. The aims were to (i) foster research cooperation between defence research actors in EU Member States, (ii) strengthen the defence industry's competitiveness and (iii) raise the level of defence technological and industrial capacity for the armed forces.

The EDA organised an EU-wide call for proposals between March and June 2016, receiving 21 submissions involving 83 participants from 20 countries. The following three projects were selected (see also **Table 7**):

- 'Inside building awareness and navigation for urban warfare (SPIDER)';
- 'Standardisation of remotely piloted aircraft system detect and avoid (TRAWA)';
- 'Unmanned heterogeneous swarm of sensor platforms (EuroSWARM)'

The pilot project paves the way for the launch of the European Commission's PADR, which, in turn, will lead to a fully fledged European defence research programme as part of the EU's next MFF (2021-2027). All of these activities (the pilot project, the preparatory action and the future European defence research programme) should support R & T⁽²⁵⁶⁾, addressing the capability priorities identified by Member States in the EDA's

⁽²⁵³⁾ European Commission communication COM(2016) 950 final.

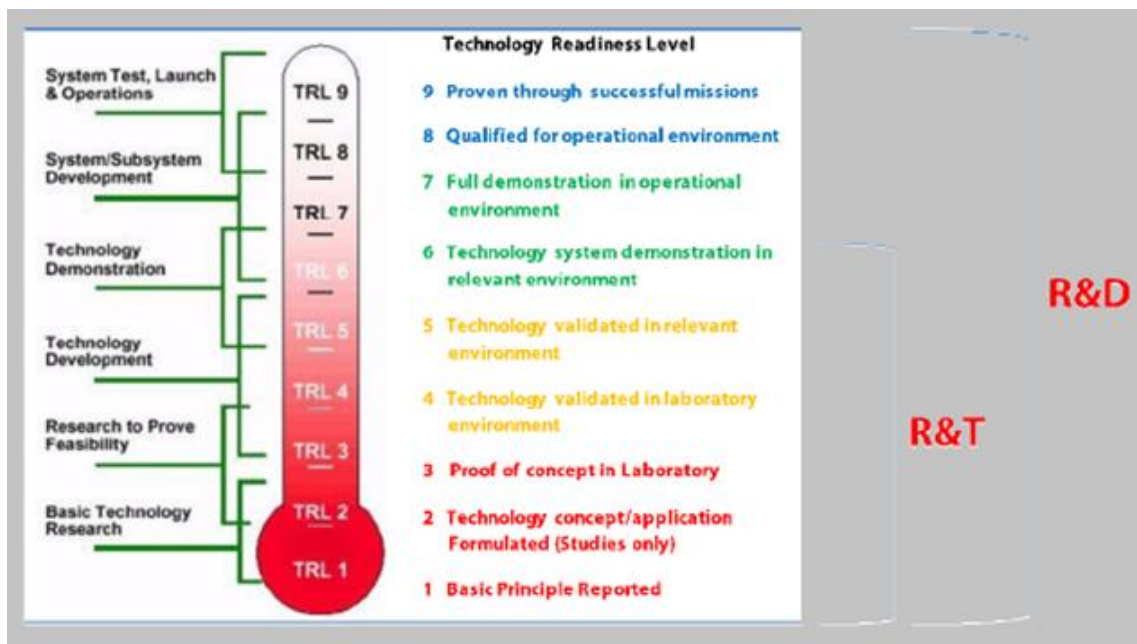
⁽²⁵⁴⁾ European Commission, 'Reflection paper on the future of European defence' (COM(2017) 315 final), Brussels, 7.6.2017.

⁽²⁵⁵⁾ Since 2004, the EDA has managed close to 200 R & T projects worth over EUR 1.1 billion; see EDA, 'EDA at a glance' (<https://www.eda.europa.eu/docs/default-source/eda-factsheets/2018-09-24-eda-at-a-glance.pdf>).

⁽²⁵⁶⁾ For definitions of R & T and R & D, see European Parliament (2016a).

Capability Development Plan; these priorities will also be taken up in future collaborative capability programmes ⁽²⁵⁷⁾. The differences between R & T and R & D are explained in **Figure 8**.

Figure 8: Differences between R & T and R & D in terms of technology readiness levels (TRLs)



Source: European Parliament (2016a), using EDA definitions for R & T and R & D expenditure.

3.2.5 The Group of Personalities (2015-2016)

Similarly to the approach adopted to security research (see Section 3.1), the European Commission set up a Group of Personalities for Defence Research in March 2015, chaired by Commissioner Bieńkowska and supported by the HR/VP Federica Mogherini. The group was composed of 15 additional politicians, academics, representatives of think tanks and representatives — mostly chief executive officers — of defence industry and research technology organisations. Its aim was to advise on how the EU could support defence research programmes.

The group presented its final report in February 2016 (EUISS, 2016), giving its views on the European context, the preparatory action and the future of defence research. The document contained nine key recommendations grouped into (i) principles, covering aspects of coordination, cooperation and governance; (ii) modalities, covering eligibility criteria, budget cover and supporting defence initiatives; and (iii) resources, setting the recommended budgets for the preparatory action and the European defence research programme post 2020. In addition, it suggested the creation of a European Defence Advisory Board, to be tasked with, among other things, advising on all aspects of the European defence action plan, giving guidance on the principles, structure and modalities of the European defence research programme and playing an active part in the creation of a European capabilities blueprint. It should also have direct access to the highest level of EU institutions during the preparation and negotiation of the next MFF.

3.2.6 The preparatory action on defence research (PADR) (2017-2019)

The EDF, launched in June 2017, was composed of two 'windows': research and capability. The research window was to fund collaborative defence research projects at EU level and was to be developed through the launch of the PADR, which would result in a dedicated EU programme in the post-2020 EU MFF. In outlining the activities under the preparatory action, the Commission took into consideration the recommendations made by the Group of Personalities in its report. The capability window, meanwhile, was to support the joint development of defence capabilities as agreed by the Member States.

⁽²⁵⁷⁾ <https://www.eda.europa.eu/what-we-do/our-current-priorities/capability-development-plan>.

The PADR was decided on by the European Commission with one main objective in mind: to demonstrate the added value of EU-funded research in the defence sector. Set to start in mid-2017 and running over a 3-year period (2017-2019), the PADR would be a test bed used to prove the relevance of European defence research and lay the foundations for a fully fledged EU defence R & D programme in the MFF 2021-2027 (EDA, 2016).

The key aspect in assessing the EU added value of the PADR would be the uptake of the technology research by the industry and ministries of defence, which would ensure the creation of new strategic capabilities for European armed forces and increase the competitiveness of the EU defence technological and industrial base.

The scope of the PADR would be decided on in consultation with Member States, the European Parliament, the EDA, the EEAS and industry. The PADR has been designed taking into account the specificities of defence-related research, including research areas and models, intellectual property rights, confidentiality of results, co-funding and rules of participation, and the role of Member States, while ensuring that is attractive for industry participants.

The focus of the PADR is on defence research rather than dual-use research. Nevertheless, it complements existing EU programmes such as FP7, H2020 and R & T activities in the Member States and in the EDA.

Following the mandate of a delegation agreement between the Commission and the EDA, signed on 31 May 2017, the Commission entrusted the EDA with the management and implementation of the research projects to be launched within the PADR, which would be done through grants awarded in EU-wide calls for proposals ⁽²⁵⁸⁾.

The budget for the PADR-related actions (EUR 90 million) is split over 3 years as follows:

- EUR 25 million in 2017 (already committed, first projects started);
- EUR 40 million in 2018 (approved and calls for proposals closed);
- EUR 25 million in 2019 (approved and call for proposals open in March 2019).

In April 2017, the Commission decision on financing the PADR and the use of unit costs for 2017 was published ⁽²⁵⁹⁾. The 2017 work programme included the following topics (further details can be found in **Table 7**).

- **A technological demonstrator for enhanced situational awareness in a naval environment.** The project aimed to show the added value of unmanned systems in enhancing situational awareness while operating alongside and communicating with other manned and unmanned systems.
- **Research in technology and products in the context of force protection and soldier systems.** This topic focused on aspects such as future generic open soldier system reference architecture; technological advancements in tailor-made blast, ballistic and CBRN protection for military personnel; and novel developments in active and passive military camouflage methods.
- **Strategic technology foresight.** The call requested the development and validation of a methodology and/or process for gathering data. These foresight activities will be carried out on a recurring basis. They will be used to develop realistic scenarios of potential future conflicts which would help in scoping EU-funded defence research.

For 2018, the PADR work programme included the following topics ⁽²⁶⁰⁾.

- **A European high-performance, trustable (re)configurable system-on-a-chip or system-in-a-package (SoC/SiP) for defence applications.** The project aims to design and validate a SoC/SiP and thus make a substantial contribution towards the development and manufacturing of European high-performance, trustable (re)configurable SoC/SiP suitable for multiple defence applications.
- **Towards a European high-power laser effector.** This topic focuses on an R & T project, followed later by a development phase, to design and build a European high-power laser effector, to become available for defence applications within the next decade.

⁽²⁵⁸⁾ EDA, 'What we do' (<https://www.eda.europa.eu/what-we-do/activities/activities-search/preparatory-action-for-defence-research>).

⁽²⁵⁹⁾ European Commission, Commission decision on the financing of the preparatory action on defence research and the use of unit costs for the year 2017 (C(2017) 2262 final), Brussels, 11.4.2017.

⁽²⁶⁰⁾ European Commission Decision C(2018) 1383 final.

- **Strategic technology foresight.** This action aims to provide an effective way of tackling the issue of the critical defence technological dependencies of the EU in relation to current and future systems and capabilities.

The 2019 PADR work programme was announced on 19 March 2019, with the following topics ⁽²⁶¹⁾.

- The first call (PADR-EMS-03-2019 ‘Electromagnetic spectrum dominance’) will result in the selection of one project for research activities at system and component levels for the development of compact, highly performing and lightweight multifunction radiofrequency systems (with a combination of radar, communications and electronic warfare functions), based on European active electronically scanned array technology, free from any non-EU nation end-user restrictions, compatible with aerial platforms and able to be integrated into other platforms. Indicative amount of the call: up to EUR 10 million.
- The second call (PADR-FDDT-EMERGING-03-2019 ‘Emerging game-changers’) will result in the funding of five projects to contribute to the development of breakthrough technologies for defence applications in the following areas:
 - low-drift, small-scale, power-efficient, integrable systems capable of delivering autonomous PNT services in GNSS denied/contested environments;
 - use of AI in defence technologies across the whole military capability spectrum;
 - use of quantum technologies for defence applications;
 - radical solutions for cost-efficient long-range precision strikes;
 - augmenting soldier capacity.

Indicative amount of the call: up to EUR 7.5 million.

- The third call (PADR-US-03-2019 ‘Unmanned Systems’) will fund one project on interoperability standards for military unmanned systems allowing interoperability of various defence units using autonomous systems. Indicative amount of the call: up to EUR 1.5 million.
- The fourth call is on future disruptive defence technologies (PADR-FDDT-OPEN-03-2019 ‘Challenging the future’); it should result in the selection of up to three projects on potential disruptive defence technologies. These projects should demonstrate (through convincing experimental proof of concept) the radical impact of technologies of any kind in the area of defence resulting in technological superiority over potential adversaries. Indicative amount of the call: up to EUR 4 million.

3.2.7 The future of European defence research: the European Defence Fund

The EDF was launched in June 2017 through a Commission communication ⁽²⁶²⁾. It will coordinate, supplement and amplify national investments in defence research, in the development of prototypes and in the acquisition of defence equipment and technology.

The EDF is expected to boost the EU’s excellence and efficiency in defence equipment and technology by supporting the whole production chain: research, prototype development and acquisition. To achieve this, the fund has two strands with different legal and funding structures, which are complementary and are being deployed gradually.

- **Research (the ‘research window’).** The EU will offer direct funding (grants) for research into innovative defence products and technologies, fully financed from the EU budget.
- **Development and acquisition (the ‘capability window’).** Member States will pool financial contributions to jointly develop and acquire key defence capabilities. The EU will offer co-financing from the EU budget to incentivise cooperation and leverage national financing.

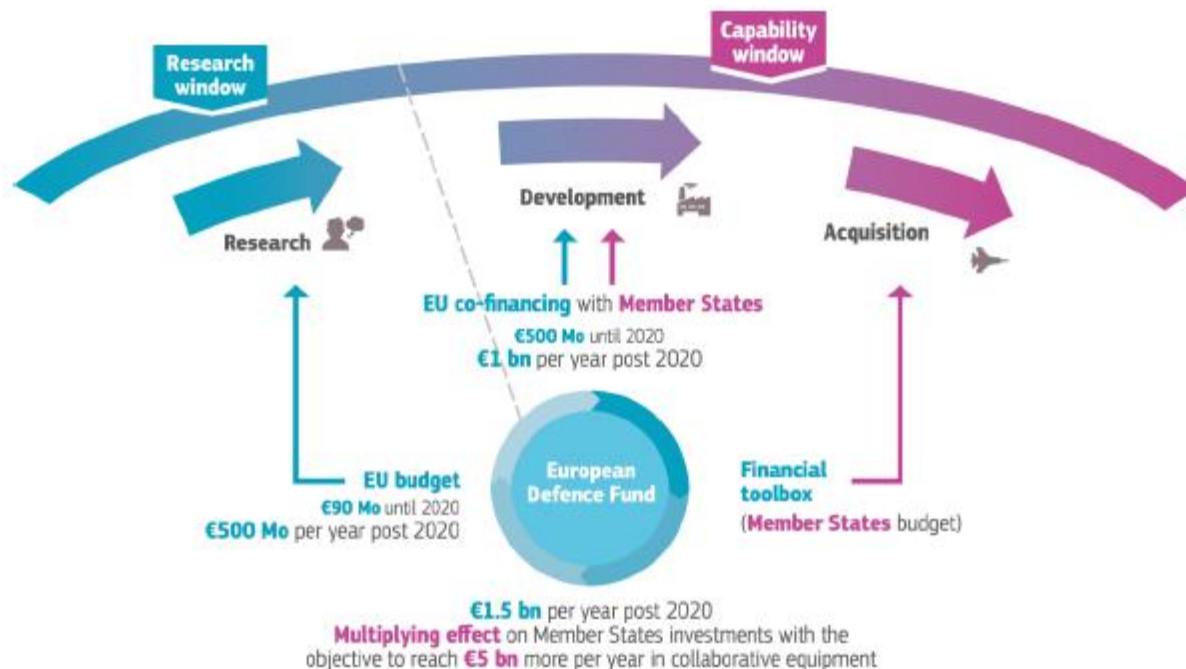
Both strands will support the priorities agreed by the Member States, notably through the *Capability Development Plan*; the Member States will also ultimately own and operate the assets.

⁽²⁶¹⁾ European Commission, Commission decision on the financing of the preparatory action on defence research and the adoption of the work programme for 2019 (C(2019) 1873 final), Brussels, 19.3.2019.

⁽²⁶²⁾ European Commission, Commission communication, ‘Launching the European Defence Fund’ (COM(2017) 295 final), Brussels, 7.6.2017.

In the period up to and including 2020, the Commission will allocate EUR 590 million to the EDF. After 2020, the Commission is proposing to allocate at least EUR 1.5 billion per year. The fund is designed not to replace Member States' defence investments but to enable and accelerate their cooperation. Taking into account Member States' contributions to finance joint development projects, the fund could generate a total investment in defence research and capability development of EUR 5.5 billion per year after 2020 (**Figure 9**).

Figure 9: Structure and details of the European Defence Fund



Source: European Commission communication COM(2017) 295 final.

Under the research window, the EU budget will fully and directly finance collaborative defence R & T activities across Europe, taking into account the defence capability and R & T priorities agreed by Member States. Priority areas could typically include critical and innovative technologies such as electronics, metamaterials, encryption software and robotics, and the research will explore future disruptive defence technologies and applications.

The Commission, in close cooperation with Member State experts and with input from the EDA, will establish annual work programmes. By delegation agreement with the Commission, the EDA will be responsible for implementing the annual work programmes by publishing the calls for proposals, organising the evaluation of project proposals and managing the research projects selected to receive EU funding.

The EDF is an unprecedented, comprehensive instrument covering funding for the whole defence industrial cycle to support European strategic autonomy. It will be launched during the next MFF period (2021-2027) and will incorporate the current PADR and European Defence Industrial Development Programme (EDIDP) ⁽²⁶³⁾, which focus on defence research and capability development, respectively. Furthermore, the Fund will include the 'Financial Toolbox', a set of standardised instruments supporting collaborative procurement projects by Member States.

For 2019 and 2020, the EDIDP has a budget of EUR 500 million and is designed to co-finance projects that contribute to excellence, innovation and competitiveness in the defence sector. The first call for proposals was launched in April 2019.

In June 2018, the European Commission presented its proposal to establish the EDF under the 2021-2027 MFF ⁽²⁶⁴⁾. The proposed budget for the period is EUR 13 billion. The fund will provide EUR 4.1 billion to directly

⁽²⁶³⁾ European Commission, 'Proposal for a Regulation establishing the European Defence Industrial Development Programme aiming at supporting the competitiveness and innovative capacity of the EU defence industry' (COM(2017) 294 final), Brussels, 7.6.2017.

⁽²⁶⁴⁾ European Commission, 'Proposal for a Regulation of the European Parliament and of the Council of the European Union establishing the European Defence Fund' (COM(2018) 476 final), Brussels, 13.6.2018.

finance competitive and collaborative research projects, in particular through grants. In addition, the EDF will provide EUR 8.9 billion to complement Member States' investments by co-financing the costs of prototype development and of certification and testing requirements.

3.2.8 The European defence research programme and Horizon Europe

In the MFF 2021-2027, the first fully fledged European defence research programme will be funded under the EDF research window, while Horizon Europe will continue funding civil security and dual-use research.

The European Commission proposed in 2018 a budget of EUR 94.1 billion, at 2018 prices, to be allocated to the Horizon Europe framework programme ⁽²⁶⁵⁾. The main aims are to strengthen science and technology, to foster industrial competitiveness and to implement the Sustainable Development Goals in the EU. Horizon Europe will introduce new features such as the European Innovation Council, missions to promote research results and new forms of partnership. Horizon Europe also aims to reduce administrative burdens and promote the concept of open science (see Section 3.1.8 for more details).

An overview of the historical evolution of European defence research and the relevant legislation is provided in **Figure 10**.

3.2.9 Other funds related to defence (2014-2020)

Currently, H2020 and the EDF (with the preparatory action and the EDIDP) are the main EU programmes for security and defence research. However, there are several more programmes that support defence research, development and innovation. The EDA is putting efforts into helping actors in the EU defence industry to find the right funding mechanisms. On its European Funding Gateway website, the main current EU funding instruments are listed ⁽²⁶⁶⁾. These are discussed hereafter.

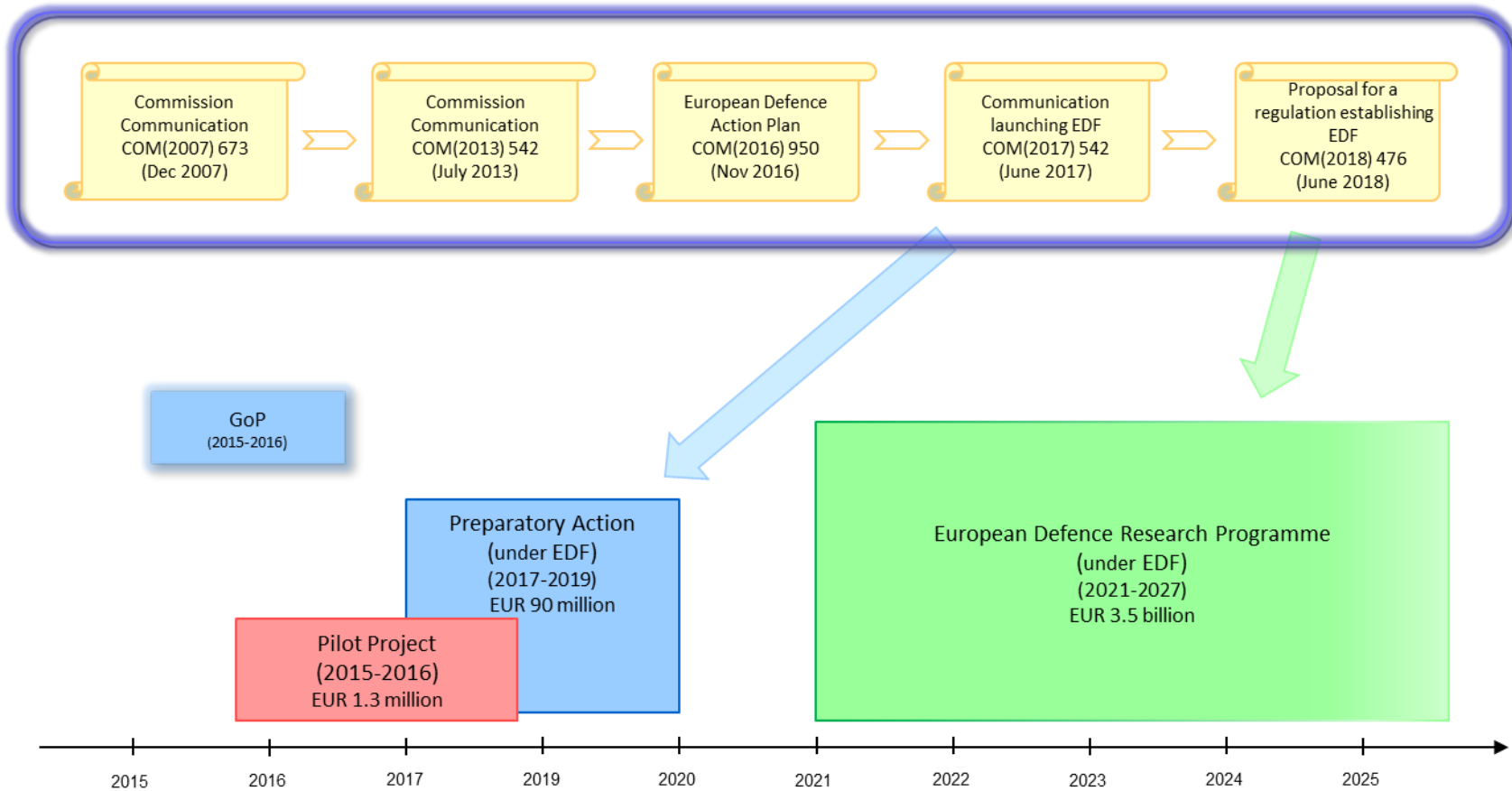
- The EDA's ad hoc projects — the EDA funds cooperative defence R & T and capability projects on a continuing basis.
- Connecting Europe Facility — through the programme facility's transport programme 'Single European sky ATM research (SESAR)', it finances cooperative projects and studies, with a focus on European transport infrastructure.
- European Structural and Investment Funds — cohesion policy:
 - the European Regional Development Fund, with the aim of creating jobs, innovation and competitiveness, can fund productive investment projects in the defence sector, projects modernising the defence supply chain, and defence and dual-use activities in R&I;
 - Interreg Europe, with the aim of achieving the European territorial cooperation goal, can fund the same type of projects of the European Regional Development Fund, but with a focus on cross-border and transnational cooperation;
 - the European Social Fund can fund projects on key skills and competences in both the defence and dual-use domains, with a focus on human capital, training and skills;
 - the Cohesion Fund can fund energy projects on climate change adaptation, the environment and resource efficiency, and public administration efficiency and capacity, with the aim of reducing disparities and promoting sustainable development.
- COSME:
 - the financial instruments under COSME (the Loan Guarantee Facility and the Equality Facility for Growth) can be used to finance high-risk SMEs working on defence and dual use;
 - COSME's work on access to market aims to internationalise SMEs, including in the defence sector.

⁽²⁶⁵⁾ European Commission proposal COM(2018) 435 final.

⁽²⁶⁶⁾ EDA, European Funding Gateway (<https://eda.europa.eu/eufunding>).

- The LIFE programme for the environment and climate action:
 - LIFE can fund pilot, demonstration, best practice and information/awareness/dissemination projects related to water, waste, energy, the circular economy, chemicals (including REACH), noise, emissions, etc;
 - The LIFE financial instruments — Private Finance for Energy Efficiency (PF4EE) and the Natural Capital Financing Facility (NCFF) — can fund innovative natural capital management pilot projects (NCFF) and energy efficiency investments and technical assistance in relation to them (NCFF and PF4EE).
- European Investment Bank — major project direct loans can fund dual-use R&T projects that are economically, financially, technically and environmentally sound and which further EU policy goals.
- Erasmus+: the scheme funds learning mobility for individuals, strategic partnerships and knowledge alliances, which are applicable in the field of defence.

Figure 10: Overview of the evolution of European Defence Research under EU funds and associated legislation



Note: GoP: Group of Personalities

Source: Authors

Table 7: Defence research projects funded using the EU budget: pilot project and preliminary action (updated in December 2018)

Programme	Acronym	Title	Objective	Budget (EUR)	Start date	End date
Pilot project	EuroSWARM	Unmanned Heterogeneous Swarm of Sensor Platforms	<p>EuroSWARM aimed to test and demonstrate that efficient and effective operation of unmanned swarm systems can bring a profound impact to the military arena. The key focus was the minimisation of uncertainties in situational awareness information for surveillance operations through a swarm system of systems composed by static and mobile heterogeneous sensors. The main objectives of the activity were to:</p> <ul style="list-style-type: none"> • develop key techniques for adaptive, informative and reconfigurable operations of unmanned heterogeneous swarm systems, namely: optimal task allocation and resource management, sensor fusion, cooperative guidance, robust sensor network; • integrate the developed enabling techniques; • validate the developed enabling techniques based on empirical simulation studies; • demonstrate the proposed solutions based on a small scale of experiments. 	430 000	28.10.2016	27.10.2017
Pilot project	SPIDER	Sensor Platform & network for Indoor Deployment and Exterior-based Radiofrequency	<p>Inside Building Awareness and Navigation for Urban Warfare: SPIDER aimed to develop an innovative system to support Urban-Warfare operations by providing improved situational awareness to operational forces entering an unfriendly building. It focused on the use of radiofrequency (RF) stationary sensors and mobile ground robots. The main objectives of the activity were to:</p> <ul style="list-style-type: none"> • develop and analyse a framework comprising the use of multiple sensors to perform indoor mapping and human detection in an Urban Warfare context; • consider the choice of a data fusion strategy to process and combine sensor data; • explore the advantages and constraints of using each solution as well as solutions encompassing autonomous robots combined with static RF sensor networks. 	430 225	22.11.2016	21.02.2018

Programme	Acronym	Title	Objective	Budget (EUR)	Start date	End date
Pilot project	TRAWA	Traffic Awareness	<p>Standardisation of Remotely Piloted Aircraft System (RPAS) Detect and Avoid: It aimed to contribute to the development of standards for a performant and affordable detect and avoid (DAA) system usable on-board Remotely Piloted Aircraft Systems (RPAS). It is focused on the Remain Well Clear (RWC) function and contributes to the standardisation activities in cooperation with other international efforts in full alignment with EUROCAE WG 105 Terms of Reference. The main objectives of the activity were to:</p> <ul style="list-style-type: none"> • specify Remain Well Clear in quantitative terms and obtain validation via simulations; • specify sensor types, detection ranges and position estimation accuracy; • develop requirements for remote pilot HMI (Human Machine Interface) characteristics. 	430 292	11.11.2016	10.05.2018
Preparatory Action	PYTHIA	Predictive methodology for technology intelligence analysis	<p>PYTHIA's main objective is to deliver a methodology for improving civil and defence technology foresight. It aims to devise an innovative methodology for strategic technology foresight, able to deliver frequent "predictions" on technology-related matters, including the discovery of major trends in a particular area of research and development. Starting from a study of the cognitive factors influencing analysts' ability to perform accurate forecasting, the project will leverage big data analytics techniques for automatically analysing large volumes of technology information collected from a wide range of publicly available sources, in order to identify future disruptive technologies and recommend themes for European defence research. The methodology will be assessed by an enlarged stakeholder group and validated scientifically and technologically in 4 workshops plus a testing session that will be organised throughout the project's lifetime.</p>	947 610	01.02.2018	31.07.2019

Programme	Acronym	Title	Objective	Budget (EUR)	Start date	End date
Preparatory Action	OCEAN2020	Open Cooperation for European Maritime Awareness	Ocean2020 supports maritime surveillance and interdiction missions at sea and to that end will enhance air, naval surface and underwater unmanned systems and integrate them into fleet operations. The information acquired will be combined with the whole set of naval info obtained by existing systems to build up a Recognise Maritime Picture of developing situations for military commanders. OCEAN2020's main objective is indeed to develop integrated system concepts that culminate in large-scale technology demonstrations for enhanced situational awareness in a maritime environment. The planned demonstrations in the Mediterranean and Baltic seas will show how innovative solutions for fusion of multiple data sources can be integrated with Combat Management Systems (CMSs) into a secure network to create a Recognized Maritime Picture. It will also show how collaborative autonomy between multi-domain unmanned vehicles can provide a force multiplier. This will provide End Users with the advantage of interoperability for joint missions and at the same time offer industry an opportunity to build Command and Control (C2) modules in a multi-company environment. To be successful in reaching these goals, the OCEAN2020 Consortium will solve the problems of integrating EU systems as well as integrating the individual organisations into a coherent team.	35 480 000	01.04.2018	31.03.2021
Preparatory Action	GOSSRA	Generic Open Soldier System Reference Architecture	GOSSRA will carry out research in the development of a Soldier System Reference Architecture ready for standardization which covers electronics, voice and data communication, software, human interface devices, sensors, and effectors. The GOSSRA study on Generic Open Soldier Systems Reference Architecture researches in the development and validation of the desired Reference Architecture by identifying trends and potentials with respect to operations and technologies; reviewing, refining and integrating the STASS I+II architectures; validating and enhancing the integrated architecture with respect to operational issues, maintenance and logistics, and technical issues; formulating the architecture for standardization; and finally technically validating, demonstrating and refining the architecture.	1 488 642	01.06.2018	31.03.2020

Programme	Acronym	Title	Objective	Budget (EUR)	Start date	End date
Preparatory Action	VESTLIFE	Ultralight Modular Bullet Proof Integral Solution for Dismounted Soldier Protection	VESTLIFE aims to develop a new lightweight and modular bulletproof integral solution, which integrates a CBRN detection system. The garments will include the possibility of an increased coverage area whilst maintaining comfort, plus a weight reduction of the ballistic panels, thus ensuring optimum balance between protection and comfort, tailoring such a protective surface to the forecasted risk mission. The project strives towards the development of different types of ballistic protection armour with advanced features in performance. This protection system will consist of different levels, mainly soft armour and hard armour. To find the optimum architecture of materials on the body, an optimum has to be found, based on both the comfort experience and the protective performance. A software model will give insights into this. This model will be used to define clothing architectures, which will be created in the integration step to validate the performance of the clothing.	2 433 425	01.05.2018	30.04.2021
Preparatory Action	ACAMSII	Adaptive Camouflage for the Soldier II	ACAMSII aims to integrate several active and passive adaptation mechanisms into a textile-based soldier camouflage system. It will address several wavelengths bands, such as visual, near infrared, short wave infrared, thermal infrared and radar. Military needs on sensing, fire power, mobility and endurance are considered. The reduction in detection range and hence the increase in survivability will be assessed using both well-established methods and new methods to capture the adaptive properties. The dialogue with military end-users will start early in the project to set requirements and continue throughout the project to ensure relevance.	2 631 507	01.05.2018	30.04.2021

Note: Projects shaded blue are financed under the pilot project and those shaded green under the PADR.

Source: EDA.

3.3 Analysis of Horizon 2020 security- and defence-related research projects

Horizon 2020, the current R & D framework programme of the EU, is the main funding tool for research projects at EU level (see Section 3.1). Its 7-year duration (2014-2020) and its multiple programmatic and thematic calls lead to the selection and funding of a vast number of projects. At the cut-off date of the present report (23 May 2018), the number of projects funded and recorded in the Cordis ⁽²⁶⁷⁾ database amounted to 16 928.

From this set, the objective was to identify those projects dealing with security and defence. The first step was to produce a list of the projects in the form of a reference master table that could be used later for various analyses. An inventory of relevant projects covering the period 2014-2018 has been carried out, allowing the production of an informative statistical analysis, such as distribution of projects per building block, core priority, Horizon 2020 programme, country involved, etc. As a consequence of the growing overlap between both civil and defence domains, the dual-use nature of projects has also been looked at.

3.3.1 Methodological introduction

The selection of relevant projects was based on a set of 34 keywords ⁽²⁶⁸⁾, which covered all themes of interest to the study, namely building blocks and priorities identified on the basis of the JRC internal strategy on security and defence and the European agenda on security. In this manner, the number of projects to be scrutinised was reduced to 5 451.

Each of these projects was then examined individually by JRC staff (a group of three reviewers) in order to decide whether to retain or reject it from the final master table. One additional criterion was used: the exclusion of all projects related solely to natural hazards, climate change, the financial crisis or purely safety-related topics. This was a consequence of the scope of this landscape report, which considers exclusively man-made risks and threats that could intentionally harm individuals and societies.

The selection or rejection of a project was assessed on the basis of its metadata available in Cordis — mainly the objective description but also the title, the H2020 programme or programmes it belongs to, the topic of the call, etc.

It should be noted that, for these reasons, not all projects belonging to H2020 Programme 3.7, 'Secure societies', were retained (decision to reject were thoroughly checked) ⁽²⁶⁹⁾, whereas selected projects could belong to programmes other than 3.7.

Additional characterisation of projects

Each retained project was then further characterised using a series of new labels answering the following thematic questions.

- Does the project belong to one or more building block, and if yes to which ones?
- Does the project belong to one or more of the three priorities in the European agenda on security, and if yes to which ones?
- What is/are the main focus or focuses of the project (i.e. deeper thematic characterisation)?
- Does the project have a dual-use potential, that is, could the research carried out in the project could be applied both in the civilian field and in the defence field?

Each project was assessed by a first reviewer and cross-checked by the two others in order to ensure consensus in the selection process. At every step of the creation of the final master table, every doubt regarding a project was considered by the three reviewers together.

⁽²⁶⁷⁾ The Community Research and Development Information Service (CORDIS) is the European Commission's primary source of results from the projects funded by the EU framework programmes for research and innovation (FP1 to Horizon 2020).

⁽²⁶⁸⁾ 'Aviation', 'border' or 'border control', 'CBRN', 'civil', 'criminal' or 'crime', 'critical infrastructure', 'critical supply' or 'critical supplies', 'customs', 'cyber', 'defence', 'disinformation', 'dual use', 'explosive', 'extremism' or 'extremist', 'fake news', 'firearm', 'hybrid', 'hybrid threat', 'maritime', 'migration', 'military', 'nuclear', 'protection', 'public space', 'radicalisation', 'security', 'smuggling', 'soft target', 'space', 'terrorism' or 'terrorist', 'threat', 'traffic', 'transport', 'war'.

⁽²⁶⁹⁾ An example of a 3.7 H2020 project not retained for the master table: 'Enhancing decision support and management services in extreme weather climate events'.

EU dual-use perspective

The interest in dual-use research, in the sense that EU legislation gives to the expression ‘dual-use item’⁽²⁷⁰⁾, is a consequence of the growing overlap between the civil and the defence domains. Military forces and defence industries rely increasingly on civil technologies and innovations, whereas civil companies are buying up technologies that are also of interest to defence enterprises (Scalia et al., 2017). Quite logically, research projects and essential technologies such as those dealing with robotics, big data and human-machine interfaces, to name just a few, will become an important source of innovation for both the civil and the defence worlds.

Although H2020 projects focus exclusively on civil applications, this does not prevent the occurrence of outputs that could lead to innovations with possible defence applications. The value of identifying those projects with dual-use potential applications is high, and this was therefore done as part of the present study. For this purpose, a report (Scalia et al., 2017) on the dual-use potential of KETs was used as a guide in deciding whether the research field of the examined H2020 project could be considered dual use or not.

The final security and defence R & D master table contains 349 projects with their original and additional metadata, gathered in an Excel file (see Annex 4). A series of analyses of these projects according to the major metadata (e.g. building blocks, priorities, funding programmes, dual-use aspects), is presented in Section 3.3.2.

3.3.2 Analysis of results

The analysis of the 349 projects related to security and defence was performed on the basis of the following criteria:

- building block;
- Commission priority (under the European agenda on security);
- main thematic focus of the project;
- H2020 funding programme;
- contributing countries — coordinator and participant;
- legal status of the participant organisations;
- dual-use potential.

3.3.2.1 Distribution of projects by building block

The building block is the first powerful discriminating classifier, and there are 11 of them in the chosen approach: border control, critical infrastructure protection, public space protection, critical supplies security, cybersecurity, CBRN-E threats, hybrid threats, combating radicalisation, countering terrorism financing, space and defence; acknowledging that they are not mutually exclusive as data show below. **Figure 11** shows the distribution of the projects by building block in quantitative decreasing order. All the data obtained from the analysis of the projects are available in Annex 5.

The most striking observation is the preponderance of cybersecurity projects, since roughly half of the projects (48 %, 167 projects) are related to this block. This does not come as a major surprise given the growing role of cyberspace in human activities, including, obviously, security.

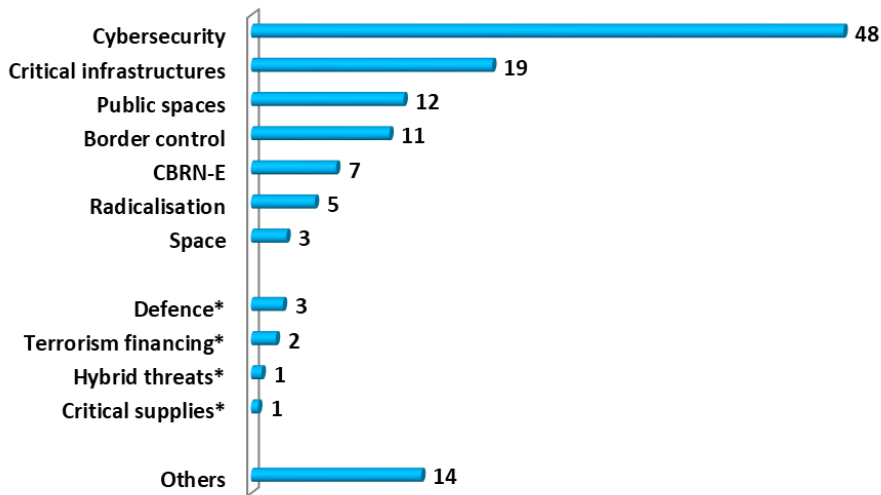
Three other blocks each account for more than 10 % of the projects, namely critical infrastructure protection (19 %, 68 projects), public space protection (12 %, 43 projects) and border control (11 %, 39 projects), all dealing with control of physical spaces and entities or making them secure.

The number of defence projects is low, which is to be expected since H2020 finances only civilian research. However, we identified several projects having an important focus on external security or peacekeeping, for instance, and thus having indirect EU defence components.

⁽²⁷⁰⁾ Council Regulation (EC) No 428/2009 defines dual-use items as ‘items, including software and technology, which can be used for both civil and military purposes, [including] all goods which can be used for both non-explosive uses and assisting in any way in the manufacture of nuclear weapons or other nuclear explosive devices’.

Some projects were not assigned to any of the building blocks and are identified as ‘Others’. They represent 14 % of the projects. Many of them deal with topics such as law enforcement problems or forensics or are theoretical studies (see Annex 4 for details).

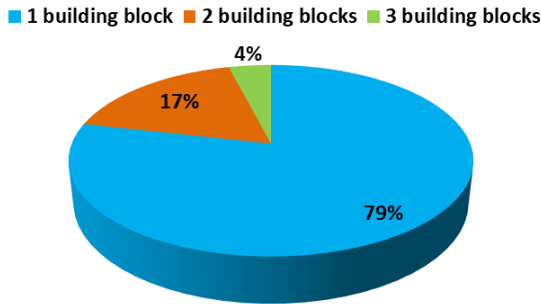
Figure 11: Proportions of projects by building block (%)



Note: *Building blocks with fewer than 10 projects.
Source: JRC analysis of Cordis data.

Whereas an overwhelming majority of projects (79 %) clearly relate to only one building block, a significant number relate to two or more blocks, as shown in **Figure 12** (why the sum of the proportions in **Figure 11** is greater than 100%).

Figure 12: Distribution of projects by number of building blocks to which they contribute (%)

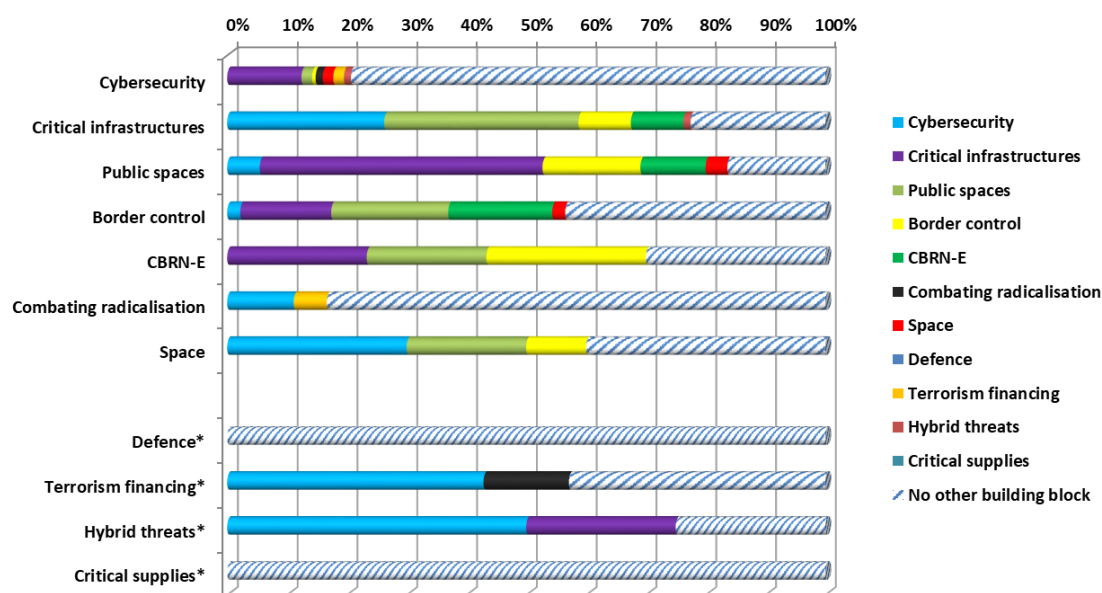


Source: JRC analysis of Cordis data.

The multi-thematic nature of many of the projects can be seen in **Figure 13****Error! Reference source not found.**, which shows how projects attributed to one particular building block (the y-axis) may also contribute to others (the composition of the horizontal bar).

It should be noted that the breakdowns displayed for the blocks with a very low number of projects (in particular critical supplies protection, hybrid threats and countering terrorism financing) have no statistical relevance and are shown only for the sake of completeness. This comment also applies to all further analysis of the data by building block.

Figure 13: Breakdown of projects by building block



Note: *Building blocks with fewer than 10 projects.

Source: JRC analysis of Cordis data.

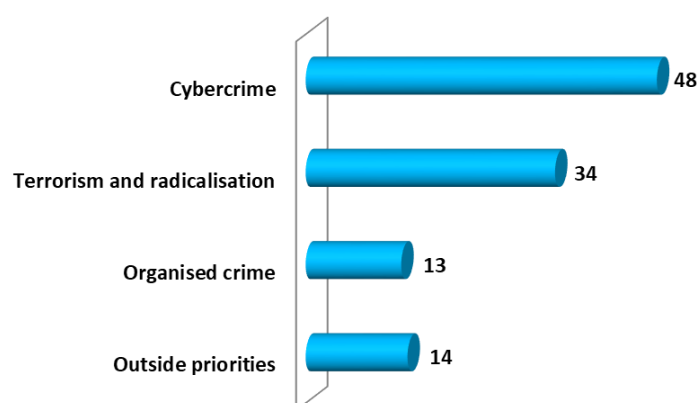
For example, out of the 167 cybersecurity projects, 21 also relate to critical infrastructures, and much smaller numbers to terrorism financing, space and public spaces, among other blocks. Other interesting interrelations are critical infrastructures and public spaces (26), border control and public spaces (9) and order control and CBRN-E (8). Projects dealing with physical entities (critical infrastructures and public spaces) appear to be the least mono-thematic.

3.3.2.2 Distribution of projects by European Commission priority

The European agenda on security established three main priorities: cybercrime, organised crime, and terrorism and radicalisation. The distribution of the 349 projects by these priorities is shown in **Figure 14**.

Roughly half of them (48 %, 169 projects) fall under the priority cybercrime, while 34 % (120 projects) and 13 % (46 projects) fall under terrorism and radicalisation, and organised crime, respectively. These figures tend again to reflect the current EU and worldwide trends: the increasing role of cyberspace and strong concerns about terrorism. In addition, 14 % (49 projects) were considered to fall outside these three priorities.

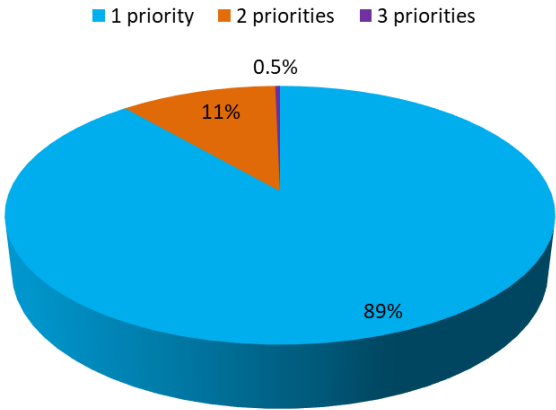
Figure 14: Proportions of projects by priority (%)



Source: JRC analysis of Cordis data.

The sum of the proportions by priority is greater than 100 %, since, as was the case with the building blocks, a significant number of projects fit under more than one priority. As shown in **Figure 15**, 89 % are related to a single priority, 11 % are related to two priorities and a negligible proportion to all three priorities.

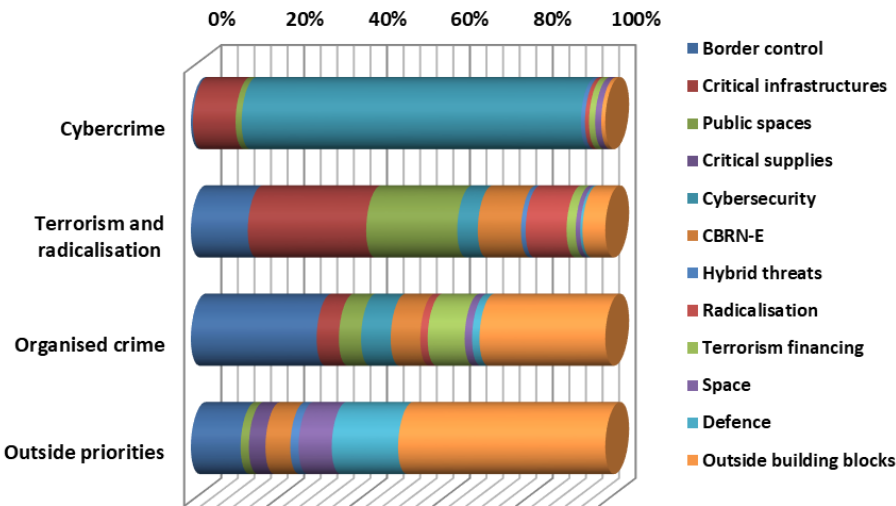
Figure 15: Distribution of projects by number of priorities to which they contribute (%)



Source: JRC analysis of Cordis data.

Combining data by building blocks and priorities as shown in **Figure 16** leads to further interesting observations.

Figure 16: Distribution of projects by priorities and building blocks (%)



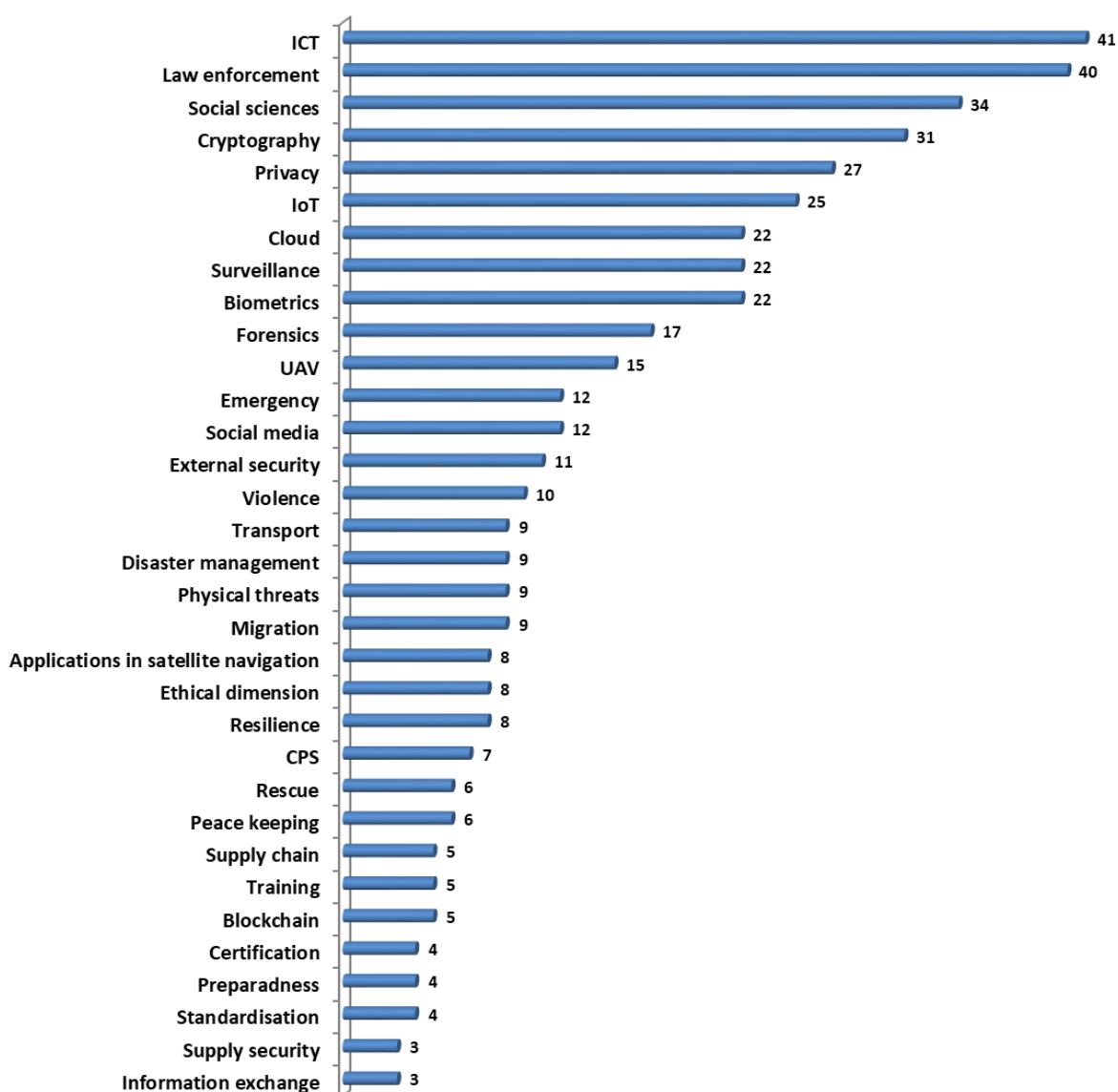
Source: JRC analysis of Cordis data.

To fight against terrorism and radicalisation, competence and hence research in many fields are needed: projects related to all blocks, although not in equal proportions, are present under this priority. When it comes to the priority of combating organised crime, projects contributing to most of the blocks are also found here, although with a much more uneven distribution: border control is, logically, at the forefront among projects to counter organised crime, and a significant amount of ‘other’ research is also involved, dealing in particular with law enforcement support, social sciences research and forensic techniques. For its part, the priority of fighting cybercrime exhibits a very different block profile: projects dealing with research in cybersecurity represent, logically, more than 80 % of projects in this area.

3.3.2.3 Distribution of projects by main focus

To go deeper than the building blocks and the priorities in characterising the projects, and in particular to provide some thematic labelling for those projects that could not be allocated to any of the building blocks or the three priorities, an additional content-related dimension, which we called ‘focus’, was introduced. A total of 33 specific focuses were assigned, such as privacy, biometrics, social media, disaster management, ethical dimension, resilience and peacekeeping, to name just a few. The full list (see in Figure 17) is certainly not exhaustive, as granularity in area identification can always be reduced. However, to maintain some statistical relevance, the lower limit was set at two having a focus in common for it to be included. In total, 80 % of the projects were labelled with one or several focuses, distributed as shown in **Figure 17**.

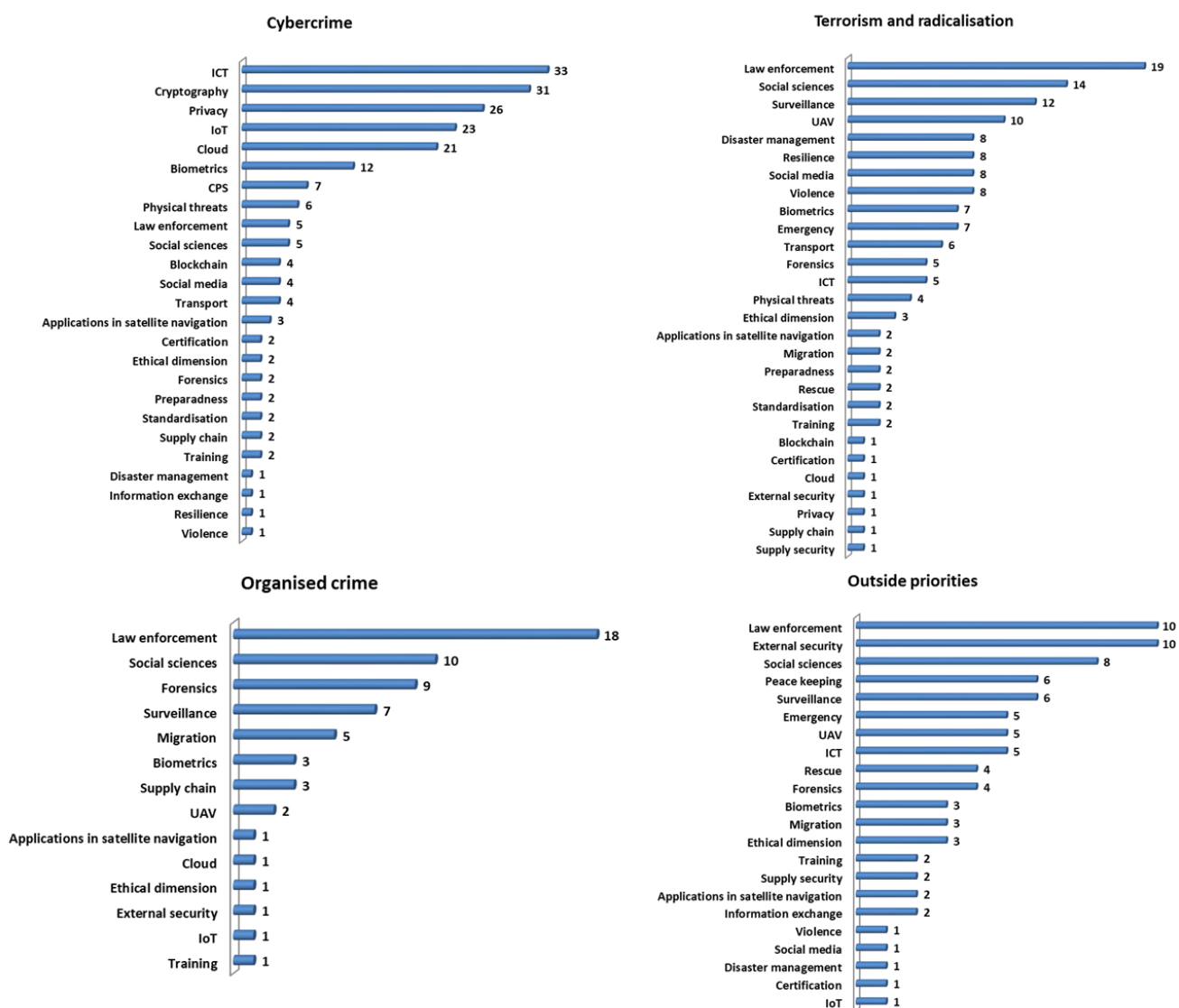
Figure 17: Numbers of projects by main focus



Source: JRC analysis of Cordis data.

Since cybersecurity is overwhelmingly the main building block, it does not come as a surprise that the predominant research focuses of the projects included ICT, cryptography, privacy, the IoT and the cloud. Details by priority are provided in **Figure 18**, which shows the projects’ major themes. Other prominent research focuses are law enforcement and social sciences, which are spread fairly evenly among the priorities.

Figure 18: Numbers of projects by priority and main focus



Source: JRC analysis of Cordis data.

3.3.2.4 Distribution of projects by Horizon 2020 funding programme

H2020 funds are structured in four main programmes, matching four priorities: (1) excellent science, (2) industrial leadership, (3) societal challenges and (4) spreading excellence and widening participation. These are, in turn, divided into further areas or subprogrammes, according to their specific objectives (**Table 8**).

For the purpose of this report, we use 'programme' to refer to each priority area and its subdivisions.

Programme 3 (H2020-EU.3) has seven specific objectives (3.1 to 3.7) on which the funding is focused (**Table 8**); these include the priority 'Societal challenges' (see Section 3.1.5 for details).

Research on security is covered by Programme 3.7, 'Secure societies — protecting freedom and security of Europe and its citizens', marked in red in **Table 8**. This objective aims to foster secure European societies in the context of unprecedented transformations and growing global interdependencies and threats, while strengthening the European culture of freedom and justice.

Table 8: Structure of Horizon 2020 funding by programme, including a breakdown of the 'Secure societies' programme (Programme 3.7, in red)

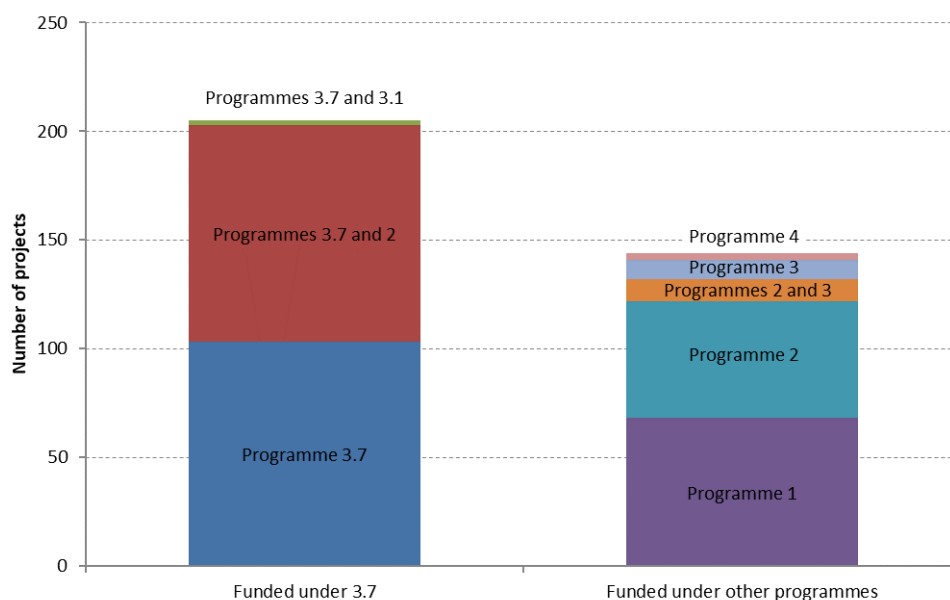
Programme	Code	Title
H2020-EU.1	1	Excellent science
H2020-EU.1.1	1.1	European Research Council
H2020-EU.1.2	1.2	Future and emerging technologies
H2020-EU.1.3	1.3	Marie Skłodowska-Curie actions
H2020-EU.1.4	1.4	Research infrastructures
H2020-EU.2	2	Industrial leadership
H2020-EU.2.1	2.1	Leadership in enabling and industrial technologies
H2020-EU.2.2	2.2	Access to risk finance
H2020-EU.2.3	2.3	Innovation in SMEs
H2020-EU.3	3	Societal challenges
H2020-EU.3.1	3.1	Health, demographic change and well-being
H2020-EU.3.2	3.2	Food security, sustainable agriculture and forestry, marine, maritime and inland water research and the bioeconomy
H2020-EU.3.3	3.3	Secure, clean and efficient energy
H2020-EU.3.4	3.4	Smart, green and integrated transport
H2020-EU.3.5	3.5	Climate action, environment, resource efficiency and raw materials
H2020-EU.3.6	3.6	Europe in a changing world — inclusive, innovative and reflective societies
H2020-EU.3.7	3.7	Secure societies — protecting freedom and security of Europe and its citizens
H2020-EU.3.7.1	3.7.1	Fight crime, illegal trafficking and terrorism, including understanding and tackling terrorist ideas and beliefs
H2020-EU.3.7.2	3.7.2	Protect and improve the resilience of critical infrastructures, supply chains and transport modes
H2020-EU.3.7.3	3.7.3	Strengthen security through border management
H2020-EU.3.7.4	3.7.4	Improve cybersecurity
H2020-EU.3.7.5	3.7.5	Increase Europe's resilience to crises and disasters
H2020-EU.3.7.6	3.7.6	Ensure privacy and freedom, including on the internet and enhance the societal, legal and ethical understanding of all areas of security, risk and management
H2020-EU.3.7.7	3.7.7	Enhance standardisation and interoperability of systems, including for emergency purposes
H2020-EU.3.7.8	3.7.8	Support the Union's external security policies including through conflict prevention and peacebuilding
H2020-EU.4	4	Spreading excellence and widening participation
H2020-EU.4.a	4.a	Teaming of excellent research institutions and low-performing research, development and innovation regions
H2020-EU.4.b	4.b	Twinning of research institutions
H2020-EU.4.c	4.c	Establishing ERA chairs
H2020-EU.4.d	4.d	A policy support facility
H2020-EU.4.e	4.e	Supporting access to international networks for excellent researchers and innovators who lack sufficient involvement in European and international networks
H2020-EU.4.f	4.f	Strengthening the administrative and operational capacity of transnational networks of national contact points

Source: European Commission.

Overall distribution

Contrary to what might have been expected — that all research projects related to security would be funded under Programme 3.7 — the analysis carried out in this study shows that a relatively high number of projects with a security component were funded under other H2020 programmes: of the 349 projects, 205 (59 %) were funded under Programme 3.7 and 144 (41 %) under other programmes (**Figure 19**).

Figure 19: Numbers of projects funded under Programme 3.7 and under other programmes



Source: JRC analysis of Cordis data.

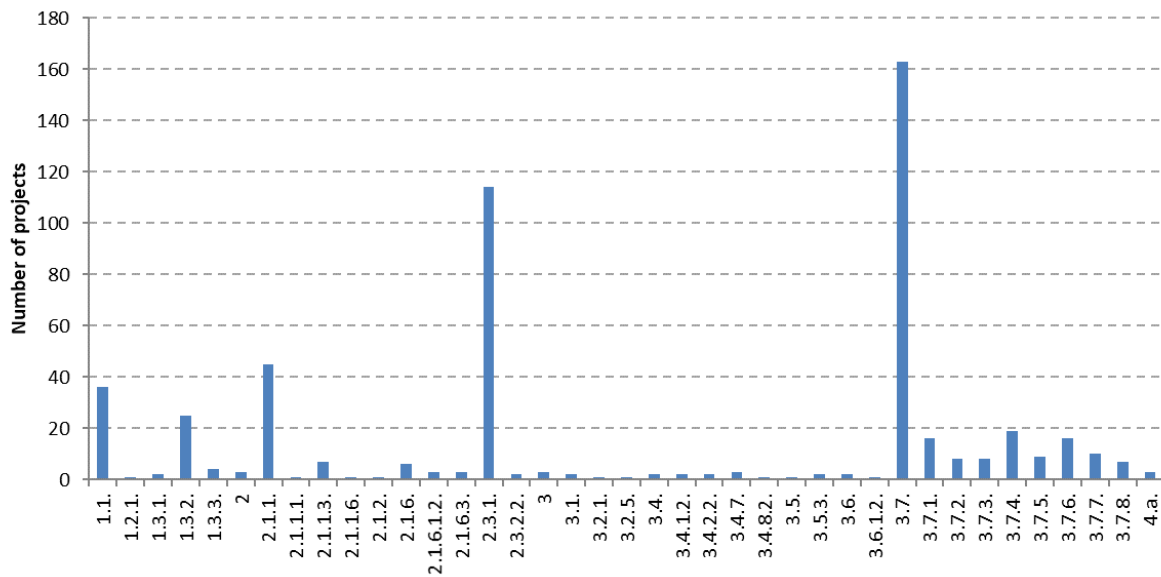
Projects funded under Programme 3.7 can be further divided into those exclusively funded under 3.7 (103 projects) and those funded under 3.7 and at least one other programme (102 projects, mainly with Programme 2).

With regard to the 144 projects not funded under Programme 3.7, almost half (68) got funding from Programme 1 ('Excellent science'), 54 from Programme 2 ('Industrial leadership') and the remaining 22 were either funded under Programmes 3.1-3.6 or from Programme 4 ('Spreading excellence and widening participation') or were co-funded under Programmes 2 and 3.

Figure 20 shows the distribution of the projects funded (or co-funded) under the various H2020 programmes in more detail. It should be noted that when a project is funded under more than one programme (e.g. under Programmes 3.7, 3.2 and 2.3), it is counted once for each of them. Therefore, the sum of projects funded under the various programmes is greater than the total number of projects.

Projects funded under Programme 3.7 dominate, but Programme 2.3 ('Innovation in SMEs') and Programme 2.1 ('Leadership in enabling and industrial technologies') finance significant shares of security research projects. It should be noted that Programme 1, which funds about 20 % of the projects, and always as an exclusive source, tends, logically, to gather projects that are oriented towards theoretical and fundamental research, whether they belong to natural/physical sciences or social sciences.

Figure 20: Numbers of projects by H2020 funding programme

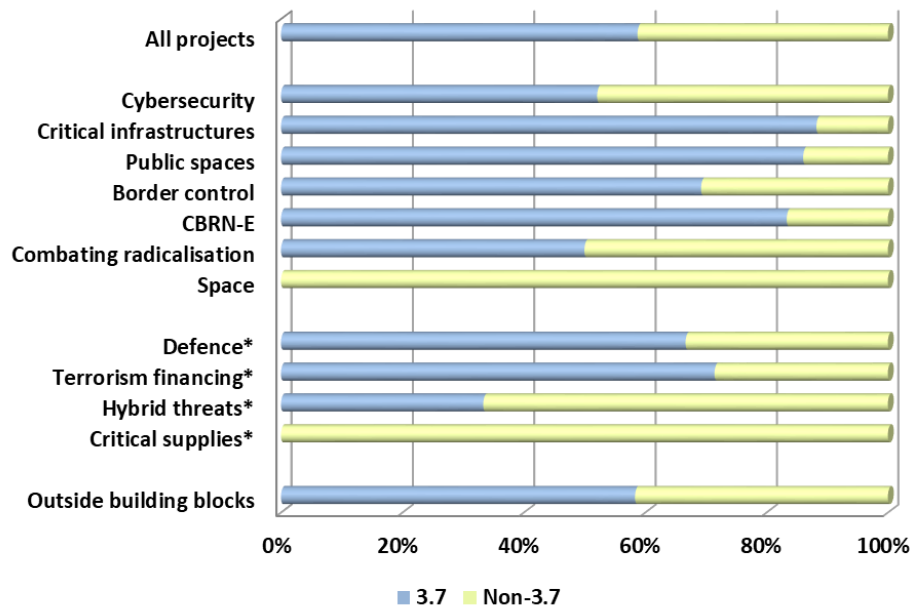


Source: JRC analysis of Cordis data.

Distribution by programme and building block

Although about 60 % of the projects were fully or partially funded under security-dedicated Programme 3.7, looking at individual building blocks brings nuance to the overall picture, as shown in **Figure 21**, where funding for each building block is divided into Programme 3.7 and non-Programme 3.7 funding.

Figure 21: Distribution of projects by building block and funding programme



Note: *Building blocks with fewer than 10 projects.

Source: JRC analysis of Cordis data.

Most building blocks with statistical relevance (i.e. including more than 10 projects) received much more than 60 % of their funding from Programme 3.7. Only cybersecurity and combating radicalisation are below the

average, with about one half of their projects funded from outside the 'Secure societies' programme, reflecting the fact that cyber matters and radicalisation concerns are far from being only security issues.

For cybersecurity, the main funding programmes outside 3.7 are 1.1 (European Research Council), 2.1.1 ('Industrial leadership') and 2.3.1 ('Mainstreaming SME support, especially through a dedicated instrument'). For combating radicalisation, the main funding programmes outside 3.7 are 1.1 (European Research Council) and 1.3.2 ('Nurturing excellence by means of cross-border and cross-sector mobility').

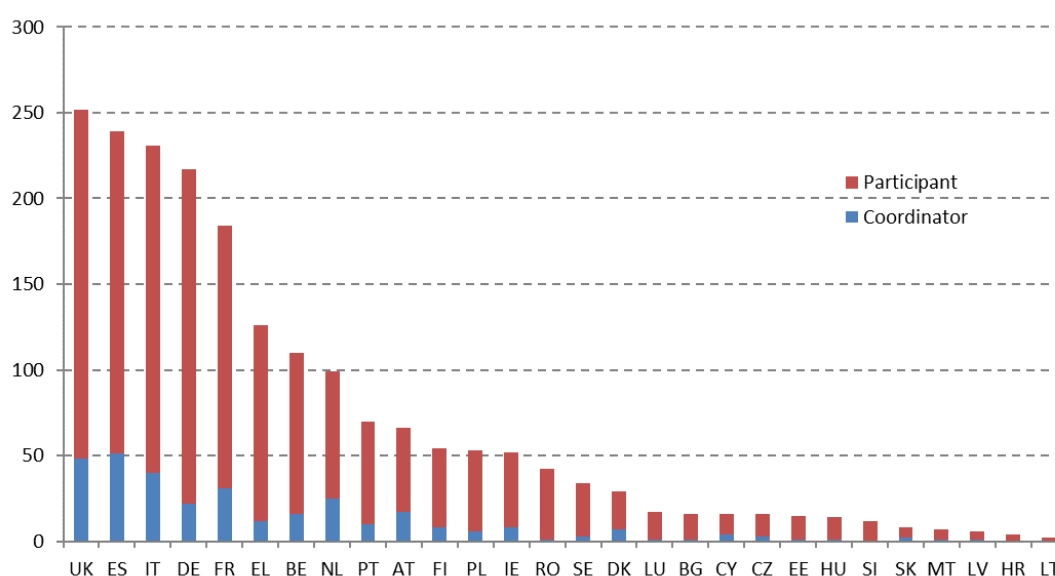
For their part, the 10 projects in the space building block were fully or partially funded under the programmes 'Leadership in enabling and industrial technologies — space' (Programme 2.1.6) and/or 'Smart, green and integrated transport' (Programme 3.4).

3.3.2.5 Distribution of projects by participant countries

Each H2020 project has one coordinating organisation (or coordinator) and may have an a priori undetermined number of participating organisations. Through these entities, there is therefore one coordinating country, while there may be several participating countries. Countries, whether EU Member States or non-EU countries, may contribute to a project through more than one organisation.

Figure 22 and **Figure 23** show the numbers of projects in which EU Member States and non-EU countries, respectively, have taken part, either as a coordinator or as a participant.

Figure 22: Numbers of projects to which EU Member States contribute



Source: JRC analysis of Cordis data.

The top five EU Member States in terms of contribution are the United Kingdom, Spain, Italy, Germany and France. They account for 56 % of the contributions of EU Member States. These are also the five largest EU Member States in terms of population. If we consider the ratio of contribution to population, the Member States making the greatest contributions are Spain, Italy, the United Kingdom, France and Germany. Considering the severe crisis that hit Greece during the past decade, its performance as the 6th biggest Member State contributor to research projects is also to be noted.

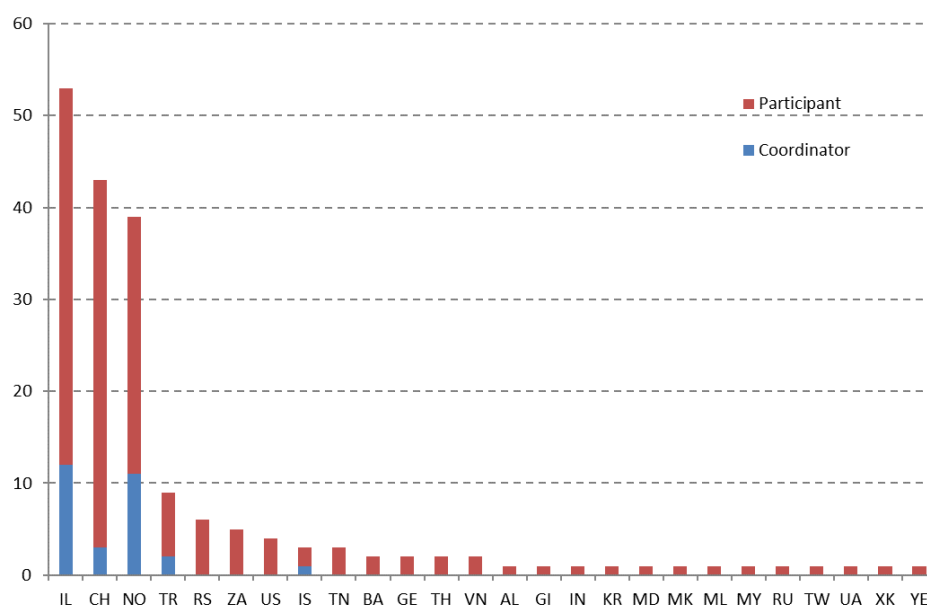
All in all, each EU Member State has contributed to security research projects.

Looking at Member States' as coordinators, it can be seen that the top five EU Member States change, with the inclusion of the Netherlands and the exclusion of Germany. The order is Spain, the United Kingdom, Italy, France and the Netherlands.

In addition to the EU Member States, 26 non-EU countries have contributed to H2020 security projects. The roles of Israel, Switzerland and Norway (53, 43 and 39 contributions, respectively) are particularly notable;

they account for 73 % of all non-EU contributions. Israel and Norway have also provided a significant proportion of project coordinators.

Figure 23: Numbers of projects to which non-EU countries contribute



Source: JRC analysis of Cordis data.

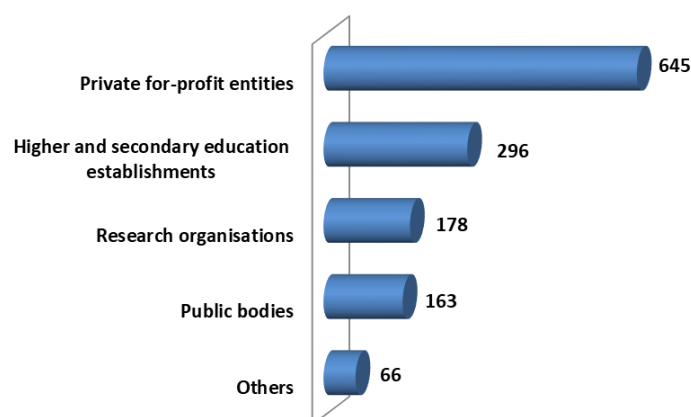
3.3.2.6 Organisations contributing to research projects: legal status

Overall consideration

Organisations that contribute to H2020 projects may have different legal statuses, being, according to the classification used by the European Commission, public bodies (e.g. ministries, public authorities and services), research organisations, private for-profit entities, or higher and secondary education establishments (mostly universities). The remaining category, 'Others', encompasses entities such as forums, foundations, NGOs and networks.

The distribution of the 1 348 organisations that contributed to the 349 security-related projects by legal status is shown in **Figure 24**.

Figure 24: Numbers of contributing organisations by legal status

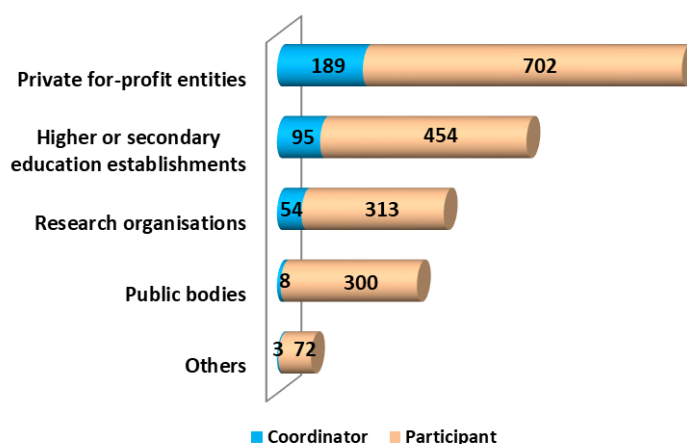


Source: JRC analysis of Cordis data.

By far the highest share is held by private for-profit companies (645 entities or 48 % of the total). It is, however, worth noting that grouping together all other statuses (703) leads to a 52 % share for (largely) public institutions/organisations and non-profit entities.

Another perspective from which to look at these data is to consider the number of contributions from the types of entities (since each entity can contribute to more than one project). This reveals that the 1 348 entities contributed to the 349 projects through 2 190 individual contributions (349 as coordinators and 1 841 as participants). The distribution of these contributions by the legal status of the entities is shown in **Figure 25**.

Figure 25: Numbers of contributions from organisations by legal status



Source: JRC analysis of Cordis data.

By far the highest share, both as coordinator and participant, is here too held by private for-profit companies (891 contributions or 41 % of the total). This means, however, that they tend to contribute less than their share of entities (48 %).

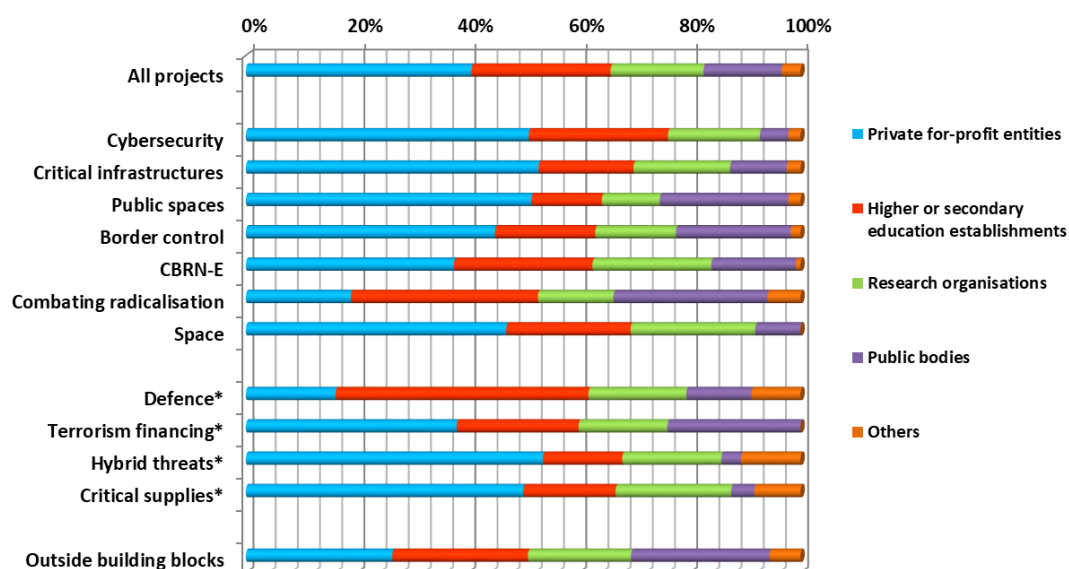
Public bodies made 308 contributions, that is, 14 % of the total. Educational establishments and research organisations made 549 (25 %) and 367 (17 %) contributions, respectively. Altogether, public and other non-profit entities made 59 % of contributions, more than their 52 % share of entities.

In terms of coordination, private for-profit companies coordinated 54 % of projects, educational establishments 27 % and research organisations 15 %. It is worth noting that the low participation of public bodies as coordinators, at only 2 %, is consistent with the political nature of most of these entities (e.g. national ministries, municipalities, police departments).

Building block and priorities perspectives on contributions

Figure 26 presents the distribution of the 2 190 individual contributions to projects according to the legal status of the contributing entities and the related building block. Annex 6 provides a list of the contributing entities with information on the building blocks and numbers of projects to which they contribute.

Figure 26: Distribution of contributions from organisations by legal status and by building block



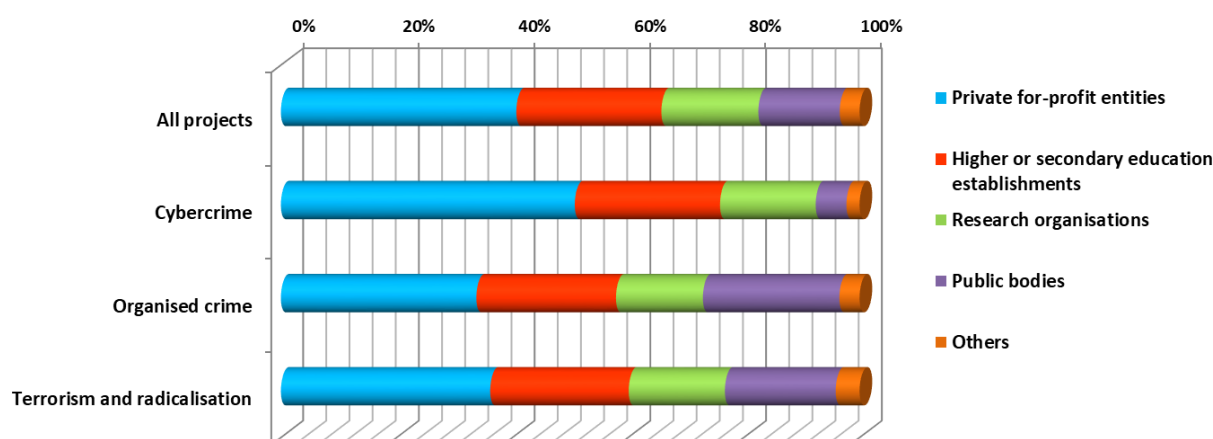
Note: *Building blocks with fewer than 10 projects.

Source: JRC analysis of Cordis data.

Comparing each block with the overall situation (marked 'All projects' in the figure), a few specificities can be observed, such as the much lower degree of involvement of private for-profit companies in projects related to combating radicalisation and the greater role of public bodies in areas such as border control, combating radicalisation and protection of public spaces. Public bodies' contribution is particularly low in the area of cybersecurity.

Figure 27 shows a similar analysis with the European agenda on security priorities as a variable.

Figure 27: Distribution of contributions from organisations by legal status and by priority



Source: JRC analysis of Cordis data.

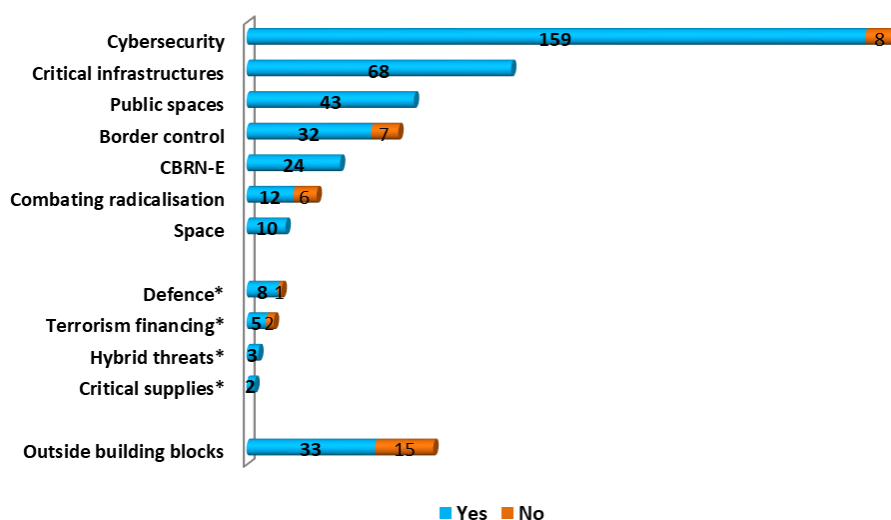
The most striking observation here, as for the analysis by block, concerns the contribution of public bodies: it is much lower than average in the fight against cybercrime, but it is much higher when it comes to countering organised crime and terrorism.

3.3.2.7 Distribution of projects by dual-use aspect

Applying the methodology described above, it appears that the overwhelming majority of the 349 security and defence research projects identified in the study were assessed as displaying dual-use potential: almost 90 % (311 projects).

Figure 28 and **Figure 29** show that, with a low degree of variability, this holds true for all building blocks (having statistical significance) and priorities, respectively.

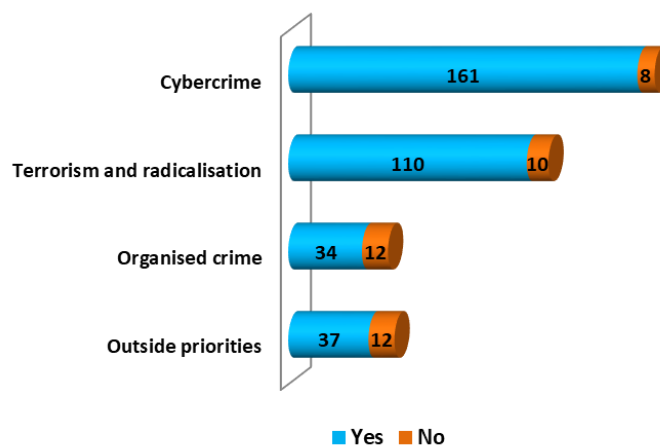
Figure 28: Numbers of projects by building block and dual-use potential



Note: *Building blocks with fewer than 10 projects.

Source: JRC analysis of Cordis data.

Figure 29: Numbers of projects by priority and dual-use potential



Source: JRC analysis of Cordis data.

The only building block and the only priority that have more than 25 % of projects with no potential dual-use applications are combating radicalisation and organised crime, respectively, which has a certain logic.

A more detailed study on dual-use projects is currently ongoing and results will be presented in the coming months.

3.4 JRC security-related research

This chapter presents research projects and stakeholders cooperation in the building blocks where the Joint Research Centre is active.

3.4.1 Border control

Since 2014, the JRC has provided technical support to DG Migration and Home Affairs on its policies regarding border control, in particular in the development of Eurosur. This system, operational since December 2013, allows the various EU Member States' competent authorities to share operational information and cooperate with Frontex and with neighbouring non-EU countries, with the goal of reinforcing control of the European southern maritime borders.

This support has been provided under three administrative arrangements between the JRC and DG Migration and Home Affairs, Marhome 1 (from January 2014 to June 2015), Marhome 2 (from July 2015 to June 2017) and Marhome 3 (from July 2017 to December 2019).

Under Marhome 3, the JRC continues to support the assessment and further development of the various components of Eurosur, with a special emphasis on the implementation of the common application of surveillance tools (Eurosur Fusion Services) and on situational pictures (National Situational Picture; European Situational Picture; Common Pre-frontier Intelligence Picture).

The JRC, in close cooperation with DG Migration and Home Affairs and Frontex, also provides support for assessing technology research and innovation for border security, including the take-up of results. Among other matters, this support can cover the exploration of innovative technology areas and components, the study of the contribution of novel solutions to the reinforcement of operational capabilities, the monitoring of readiness levels of technologies under development and assessment of R & D project results in relation to user needs.

CISE for maritime surveillance⁽²⁷¹⁾ is one of the pillars of the EUMSS (see Section 2.1.4.1) and plays a pivotal role in the protection of the EU's borders at sea.

CISE aims to create a political, legal and technical environment to enable the automatic exchange of maritime surveillance information between relevant maritime authorities in the European Economic Area member countries from different communities/sectors: maritime safety, security and pollution prevention; fisheries control; pollution response / the environment; customs; border control; general law enforcement; and defence.

CISE is now entering a transitional phase, which will lead to its becoming operational by the end of 2020.

The JRC has played a crucial role in providing scientific and technical advice to DG Maritime Affairs and Fisheries and Member States since 2010. In close collaboration with experts from Member States, it has developed and maintains the CISE data and service models, which are the key interoperability tools for enabling the information exchange among the different communities; they could be repurposed to enable such interoperability among the many different systems involved in border control.

Figure 30 provides a more detailed overview of the JRC's work in the area of border control, organised by topic, action and deliverable.

⁽²⁷¹⁾ European Commission, Commission communication, 'Towards the integration of maritime surveillance' (COM(2009) 538 final), Brussels, 15.10.2009.

Figure 30: Overview of JRC actions and deliverables in the area of border control, 2018

topics	actions	deliverables
Information exchange for smarter border control	Stronger and smarter information systems for borders and security	<ul style="list-style-type: none"> • Anti-fraud information system (AFIS). Verification of customs import declarations (SAD). Container Status Messages (CSM) • FRONTEX Media Monitor (FMM). Collection, classification and dissemination of Open Source Information
	Improving mobility and efficient border crossing	<ul style="list-style-type: none"> • ConTraffic Visual Analytics. Flows of shipping containers • Applicability and usefulness of ConTraffic data. Up-to-date situation awareness information • Knowledge and capabilities for securing supply chains. Improve customs risk management • Future Import Control System (ICS2). • Customs data analysis for anti-fraud • European Travel Information and Authorisation System (ETIAS). Mobile app to access to the ETIAS
	Action Plan to strengthen the European response to travel document fraud	<ul style="list-style-type: none"> • Schengen Master List system • Chains of trust leveraging on soft ID mechanisms • Operational Systems for Securing Borders, Migration and Asylum
	Simplify registration of refugees and other migrants	<ul style="list-style-type: none"> • Issuance and interoperability of the EU Laissez-Passer • Biometric registration of migrants (including children) in support to EURODAC • Devices for fingerprint acquisition
Border surveillance	Reducing the death toll at sea	<ul style="list-style-type: none"> • Best practice guidelines for age assessment of children in migration • Chairing and managing of the Technical Advisory Group for Maritime Surveillance • Test bed platform for the Common Information Sharing Environment for the Maritime Domain (CISE)
	Situational awareness and reaction capability at the external borders	<ul style="list-style-type: none"> • CISE Data and Service model. Connecting Europe Facility digital building blocks • Common Application of Surveillance Tools (EUROSUR Fusion Services)
	Migration flows towards the EU	<ul style="list-style-type: none"> • Assessing technology research and innovation for border security • Data about children in migration. Data Hub for children in migration • Migration inclination indexes • Migrant communities in EU • Skill matching and migration • Structural Migration Profiles (MP). Atlas of Migration • Migration and the labour market • Pressure conditions on the asylum system of EU Member States. Composite indicator Asylometer
	Fight against trafficking of human beings and migrants smuggling networks	<ul style="list-style-type: none"> • Children in migration • Migrants, refugees, conflicts and security
Aviation security screening equipment	Compliance of explosive trace detection	<ul style="list-style-type: none"> • Europol Media Monitoring. Combating organised crime, terrorism and serious crimes. • Supporting EU-wide control of explosive precursors
	Automated explosives detection x-ray screening equipment	<ul style="list-style-type: none"> • Explosive trace detection (ETD) in EU airports. Aviation security inspectors, test kits, testing methods and training
	Handheld detection equipment used in the frontline	<ul style="list-style-type: none"> • Detection performance of x-ray screening equipment in the field. Explosive detection systems for hold and cabin baggage
	Opening up JRC experimental facilities	<ul style="list-style-type: none"> • Testing of ETD equipment at European test centres (ECAC)
Cross sector application of screening and detection security technology	Aviation screening and detection technologies for other transport modes	<ul style="list-style-type: none"> • Recommendations for Harmonised Routine Testing of Aviation Security Equipment • Aviation screening and detection technologies and methodologies to other modes of transport and soft targets
	Synergy between screening and detection technologies and protection of buildings and soft targets	<ul style="list-style-type: none"> • Field testing of security equipment and procedures

Source: Authors.

3.4.2 Critical infrastructure protection

In support of EU efforts to protect critical infrastructures, the JRC coordinates ERNCIP, a framework for sharing knowledge and expertise for better protection of critical infrastructures against all types of hazards; provides technical support for the review of the directive on ECI; and carries out various research activities such as the development of methods and tools for international cybersecurity exercises, an assessment of the vulnerability of networked infrastructures in case of extreme space weather events, and an evaluation of the resistance of buildings and transport systems to explosions.

Figure 31 provides a more detailed overview of the JRC's work in the area of critical infrastructure protection, organised by topic, action and deliverable.

Figure 31: Overview of JRC actions and deliverables in the area of critical infrastructure, 2018

topics	actions	deliverables
Understanding complexity and interdependencies of infrastructures and services	Geospatial Risk and Resilience Assessment Platform (GRRASP) assistance to MS to identify interdependencies of infrastructure and improve preparedness (what-if scenarios)	<ul style="list-style-type: none"> European Resilience Management Guideline on implementation of organisational, societal and technological resilience to CI, EU risk assessment guidelines and operators workshop Visual analytics and tools for resilience (large scale complex networks, incl. CI & social networks); links between tools (GRRASP, Exito, Narrator...) Further develop GRRASP for assessing interdependencies and CI impact at MS scale
	Network analytics use-case to pan-European infrastructures (vulnerability)	<ul style="list-style-type: none"> European Resilience Management Guideline on implementation of organisational, societal and technological resilience to CI, EU risk assessment guidelines and operators workshop Visual analytics and tools for resilience (large scale complex networks, incl. CI & social networks); links between tools (GRRASP, Exito, Narrator...)
Innovative security solutions and guidance to MS and security community	ERNCIP activity (European Reference Network for Critical Infrastructure Protection) in security (anticipation, fast reaction, hybrid threats). Quantum technology	<ul style="list-style-type: none"> Further develop GRRASP for assessing interdependencies and CI impact at MS scale ERNCIP in existing areas of high priority and emerging issues: standardisation, vulnerability indicators and methods to assess hybrid threat vulnerabilities ERNCIP guidance in security of large scale infrastructures, standardisation in EPCIP and CBRNE; inventory of labs ERNCIP recommendations for future research and standardisation in CBRNE
	Gaps and security solutions in RN threats detection; chemical and biological threats; explosives (securing large areas and explosives effects)	<ul style="list-style-type: none"> Further develop GRRASP for assessing interdependencies and CI impact at MS scale Urban information and analysis for humanitarian and recovery interventions (Syrian cities) ERNCIP recommendations for future research and standardisation in CBRNE Crisis/security monitoring and mapping products in Global Crisis Atlas Internet Topology Portal Application for EEAS (CoOL, Consular OnLine) for information exchange and cooperation in major crises In CI: best practices and guides for protection and resilience for threats (natural hazards, CBRNE, terrorism); training programmes for MS; gaps; a "one stop shop" analysis centre for MS Geospatial technologies for Peace and Stability: Global Conflict Risk Index model, Conflict Resilience indicator; Global Crisis Atlas (emerging threats); Geospatial Conflict Intelligence ("PEACE" platform) Models & simulation tool to assess vulnerability of existing buildings and other soft-targets concerning explosives effects ERNCIP guidance in security of large scale infrastructures, standardisation in EPCIP and CBRNE; inventory of labs
MS capacity for current and emerging threats	Online training platform on security and resilience for MS	<ul style="list-style-type: none"> ERNCIP guidance in security of large scale infrastructures, standardisation in EPCIP and CBRNE; inventory of labs Training module in GRRASP for policy makers; training for MS
	Risk assessment for critical infrastructure (CI) (incl. resilience) for MS	<ul style="list-style-type: none"> Visual analytics and tools for resilience (large scale complex networks, incl. CI & social networks); links between tools (GRRASP, Exito, Narrator...) European Resilience Management Guideline on implementation of organisational, societal and technological resilience to CI, EU risk assessment guidelines and operators workshop
	Develop network of operators across sectors	

Source: Authors.

3.4.3 Public space protection

The JRC is actively involved in the implementation of the action plan on protecting public spaces. Its main actions are as follows.

- It is developing guidance material, for example on the protection of buildings against terrorist attacks, and promoting the concept of ‘security by design’. The first guideline for the protection of city centres using barriers has recently been issued (Karlos et al., 2018a).
- The JRC provides training for local authorities aiming to enhance urban security ⁽²⁷²⁾.
- It has been working on fostering standardisation in the field of public space protection, for example by testing security barriers against vehicle ramming or windows against blasts.
- It carried out a technology review to identify threats and new protection techniques.
- The JRC supports horizon scanning and the assessment of emerging threats.

Figure 32 provides a more detailed overview of the JRC’s work in the area of public space protection, organised by topic, action and deliverable.

Figure 32: Overview of JRC actions and deliverables in the area of protection of public spaces, 2018-2019

topics	actions	deliverables
Protection of buildings against terrorist attacks	Guideline for protection of buildings against terrorist attacks. Elaborate possible extension to protection of structures against military attacks and provision of standards for military purposes	<ul style="list-style-type: none"> Tools for numerical simulations and experimental evidence to assess vulnerabilities, investigate protection solutions, and technical guidance Design of explosions effects assessment tool
	Training material and events for MS building security officials and practitioners	<ul style="list-style-type: none"> Cooperation with DG HOME and the MS to mitigate risks and exchange of know-how and guidance material
	Protection of EC buildings	<ul style="list-style-type: none"> Numerical simulations and case-specific studies
Protection by urban planning – new buildings and public areas	Mapping experiences concerning barriers; state of the art of existing protection solutions, dedicated workshops/ training on protection	<ul style="list-style-type: none"> Development of the security by design concept.
Manage knowledge on the protection of humans	Catalogue on existing guidance material on humans protection	
	Effects of fragments impacting humans and of blast waves; new materials for body armour	<ul style="list-style-type: none"> Dual-use technologies for blast protection of public spaces
Involving civilians in the protection through dissemination of information, guidelines and better use of ICT	Information material, approaches and tools to work with the public	
	Development of safety and security mobile apps for direct citizens’ use, awareness and involvement in self-protection	

Source: Authors.

⁽²⁷²⁾ As an example, a training session on protection of public spaces and vehicle attack and blast mitigation was organised by the JRC in June 2019; see European Commission, ‘Protection of public spaces, vehicle and blast mitigation — hands on training and exchange of best practices, JRC Ispra, 12-13 June 2019’ (<https://ec.europa.eu/futurium/en/security-public-spaces/protection-public-spaces-vehicle-and-blast-mitigation-hands-training-and>).

3.4.4 Critical supplies security

In 2016, the JRC finalised a report, *Raw Materials in the European Defence Industry* (Pavel and Tzimas, 2016), which was used and quoted in drafting the European defence action plan. A new administrative arrangement is currently ongoing with DG Internal Market, Industry, Entrepreneurship and SMEs with the objective of identifying bottlenecks and supply risks linked to raw materials and advanced materials included in dual-use technologies in Europe. The technologies considered are batteries; fuel cells and hydrogen storage; robotics; drones; additive manufacturing (3D printing); and electronics.

In 2017, the JRC provided the methodology and the guidelines for assessing the most recent EU list of critical raw materials, published every 3 years by the European Commission (as a communication). The main novelty is related to an increased number of factors supporting criteria behind the security of supply, which include import dependency, trade barriers and additional socioeconomic and environmental impacts.

The JRC has also supported DG Trade and DG Internal Market, Industry, Entrepreneurship and SMEs with trade-related information on raw material products used in negotiating free trade agreements on behalf of the EU.

These activities are continuing during 2019-2021, with the 2020 EU list of critical raw materials being assessed by the JRC and specific information on raw materials and trade in relation to 31 non-EU countries being provided for EU future negotiations on free trade agreements.

Figure 33 provides a more detailed overview of the JRC's work in the area of critical supplies security, organised by topic, action and deliverable.

Figure 33: Overview of JRC actions and deliverables in the area of critical supplies, 2018-2020

topics	actions	deliverables
Raw materials supply risks for EU's industry	List of critical raw materials (considering import dependency, trade barriers and socio-economic environmental impacts)	<ul style="list-style-type: none"> Further development of: knowledge on the critical raw materials supply chains (incl. technologies for dual-use and products for defence industry); information and standardization aspects on secondary market. Analysis of stocks of raw and secondary raw materials. Mitigation of supply risks Development of trade knowledge and indicators re. to EU MS and third countries in RMIS's Economics and Trade tile. Science for Policy study on impacts on EU economy of trade barriers by third countries to selected raw materials and to products supply chains
	List of Raw Materials in the European Defence Action Plan used for developing key defence capabilities (Identifying bottlenecks and supply risks)	<ul style="list-style-type: none"> Further development of the EC Raw Materials Information System (country profiles, raw materials profiles and gateway to knowledge providers and to secondary and critical raw materials)
Illegal trade of non-food non energy raw materials (conflict minerals, i.e diamonds)	Work in area of diamonds (potentiality for more conflict minerals) (separate section of EU Raw Materials Information System RMIS)	<ul style="list-style-type: none"> Management and monitoring of Kimberley Process Certificate Scheme's certificate Forecasting illicit diamond pits by satellite imagery in selected countries
	Work in area of other conflict minerals (3TG)	<ul style="list-style-type: none"> Case study to explore conflict minerals and materials used in batteries in the context of social and environmental considerations associated to their raw materials supply chains.
Standardisation of dual use products (intensive in critical raw materials use) along their supply chain	Support to GROW, CEN/CENELEC in ICT products containing CRMs and other with high potential of end-of-life improvements (recyclability, durability)	<ul style="list-style-type: none"> New standards to enhance resource efficiency (measurement of material efficient recycling of products to maximise output of secondary raw materials)
Energy fuel raw materials – EU resilience to energy supply	Evolution of material demand; identification of the supply chain; supplier countries; competing energy markets; weakest supply chain links; EU resilience; materials issue for infrastructure and interactions with the energy sector and Defence sector. Maintain databases and view on fuel storage, inventory, and consumption patterns	<ul style="list-style-type: none"> Unconventional hydrocarbons - energy security, technological, economic and policy aspects (incl. stakeholder engagement). Hydraulic fracturing and alternative fracturing technologies. Power system regional market and security analyses in Central-South Europe, Baltics and in regions of the Mediterranean area (considering market integration and energy security challenges linked to EU's climate policies and initiatives implementation). Support to EU policy on Risk Assessment for the Security of Electricity Supply EU gas market (data sources regarding gas demand and prices in the EU). State of implementation of EU legislation in specific MS and Energy Community countries Establishment of a European Energy Atlas (EURENA) (visualization of resources, installations and other related information of the European energy portfolio) Indicator framework to assess resilience of critical energy infrastructure (incl. targets of the Energy Union, diversification of sources of supply, distributed generation capacity, cross-border interconnections, natural hazards, cyber-attacks) Implementation of Regulation (EU) 2017/1938 on safeguard the security of gas supply: regional Risk Assessments and Plans by MS; support to MS; support to analyse situation of specific MS, Energy Community contracting parties and gas suppliers; and guidance and best practices. Potential of the flows of lost resources to produce secondary raw materials Further development of the EC Raw Materials Information System. Biotic materials

Source: Authors.

3.4.5 Cybersecurity

The JRC is currently involved in various scientific and technical activities supporting other DGs' tasks. Significant examples are listed hereafter. Together with Connect, the JRC is active in particular in:

- exploring new means of embedding the concept of privacy and security by design into digital services, mobile devices and the IoT;
- empowering citizens in protecting their digital security and privacy;
- establishing and supporting the contractual public-private partnership for the cybersecurity industry;
- exploring cybersecurity issues related to emerging e-payment systems (crypto-currencies) and new cutting edge paradigms for e-services (distributed ledgers);
- supporting the establishment of the European Cybersecurity Industrial, Technology and Research Competence Centre ⁽²⁷³⁾, by publishing a cybersecurity landscape mapping (Bordin et al., 2017), then a taxonomy and classification scheme aligning cybersecurity terminologies, definitions and domains (Nai-Fovino et al, 2018a), as well as an identification and mapping of EU cybersecurity centres (e.g. research organisations, operational centres) according to their specific expertise, using the proposed taxonomy (Nai-Fovino et al, 2018a).

The JRC, together with DG Migration and Home Affairs, works to:

- develop digital forensic techniques as a contribution to the EU agenda for security;
- increase the security of the external borders (e.g. helping to design and implement the EU Entry–Exit System, thus contributing to the protection of the external borders and the effective processing of Schengen visas);
- strengthen the capacity of Frontex to carry out border controls, risk analysis and joint operations at the external borders;
- provide scientific support to strengthen large EU information systems, including for the free movement of citizens (e.g. work on interoperability, new biometric arrangements, residence permits, digital identity management, smart card security, etc.).

In the field of energy, the JRC is cooperating with DG Energy on putting in place sustainable structures, tools and procedures for a secure system of digital exchanges between Euratom Safeguards, EU nuclear operators, Member States and, possibly, the IAEA. The JRC also contributes to cybersecurity and privacy in the energy sector by facilitating the energy transition through smart grids and smart home applications, and by studying the application of the virtual currency and distributed ledger paradigms to create a seamless internal energy market.

As far as transport is concerned, the JRC collaborates with DG Mobility and Transport on activities such as:

- intelligent transport systems and electronic tools, providing technical support to implement the 'smart tachograph';
- development of cooperative intelligent transport systems and connected automated vehicles (including vehicle cybersecurity);
- development of electronic tools in support of quality inland water transport across Europe.

Figure 34 provides a more detailed overview of the JRC's work in the area of cybersecurity, organised by topic, action and deliverable.

⁽²⁷³⁾ <https://ec.europa.eu/digital-single-market/en/european-cybersecurity-industrial-technology-and-research-competence-centre>; consulted on 28 January 2019.

Figure 34: Overview of JRC actions and deliverables in the area of cybersecurity, 2018

topics	actions	deliverables
Important actor in CS package implementation	Mapping CS competences, governance proposals & economic analysis for European Cybersecurity Research & Competence Centre	
Follow up priority actions from roundtables	Mapping CS actors (JRC & outside); CoP; Horizon scanning	
CS in industrial and service sectors and digitised environment	EU framework for security certification & labelling (ICT products and services)	<ul style="list-style-type: none"> Clustering CS industry domains; standardisation and labelling
	Emerging threats to network and software security and mitigation measures	<ul style="list-style-type: none"> Mobile environments and IoT: online tracking, mobile and cloud based applications, IoT: Smart-House, Smart-buildings and Industry 4.0 (incl. standardisation) Privacy protection of Over-the-Top services: email security, web tracking (Do-Not-Track technologies for consent models); end-user perceptions on IoT Network CS: new Internet attacks (cloud, mobile, SCADA etc.). IT experimental facilities (OpenSpace & EPIC labs)
	CS for Intelligent Transport System (C-ITS)	<ul style="list-style-type: none"> Security and Privacy/Data protection challenges: exposure to disruptions, assessing impacts, and mitigation measures Digital tachographs security and interoperability: requirements for certification and reliable readers; vehicles weight and professional drivers monitoring Smart Tachographs regulation implementation (Root Certification Authority and single EU Interoperability certification laboratory) Electronic Tools for Inland Waterways Transport New Security Certification Policy and EU infrastructure for C-ITS (EU I-ITS Credential Management System) Interoperability Certification of Digital Tachograph (DT), Smart Tachograph cards and vehicle units
	Energy CS strategy	<ul style="list-style-type: none"> Interactions between smart-house devices, smart-metering systems and smart-grids; Energy CS Strategy establishment and Energy Network Code definition for CS; Distributed Ledgers use in micro Generation Distributed Ledgers in DSM: opportunities and policy options (energy use-case) CS landscape Nuclear safeguards: interactions Euratom services-stakeholders; protected transmission of classified digital documents
	Digital identities in DSM	<ul style="list-style-type: none"> Privacy protection of Over-the-Top services: email security, web tracking (Do-Not-Track technologies for consent models); end-user perceptions on IoT Trust chains in issuing identity and travel documents, softID and traditional documents Laissez Passer Smart-Borders: Schengen Master List operational system (digital certificates for electronic passport authentication); mobile apps for ETIAS (European Travel Information & Authorisation System)
	Selected industrial services/ sectors (finance, transport, eHealth, nuclear, security screening and detection equipment, eGovernment)	<ul style="list-style-type: none"> Anti-money laundering policy package (virtual-currencies and distributed ledger technologies) Security and interoperability of digital tachographs: requirements for certification and reliable readers; vehicles weight and professional drivers monitoring Nuclear safeguards: interactions Euratom services-stakeholders; transmission of classified digital documents New Security Certification Policy and EU infrastructure for C-ITS (EU I-ITS Credential Management System) Privacy protection of Over-the-Top services: email security, web tracking (Do-Not-Track technologies for consent models); end-user perceptions on IoT Automatic Fingerprint Identification System (AFIS) implementation, SIS revision (face recognition and tattoo image content retrieval systems); organised crime disruption with digital technologies (forensics) Fingermarks in Schengen Information System (SIS)
	Cyber-awareness, training and education	<ul style="list-style-type: none"> Happy Onlife software (safe ICT use for adults and children); CS awareness (education and behavioral assessment; cyberbullying to children) Privacy protection of Over-the-Top services: email security, web tracking (Do-Not-Track technologies for consent models); end-user perceptions on IoT CS landscape
Digital forensic techniques and information systems for law enforcement	Digital forensic techniques (e.g. encryption)	<ul style="list-style-type: none"> Fighting cybercrime: new vehicles and digital payments fraud Child Sexual Abuse (CSA) online (identification of authors and victims) Organised crime disruption HPC Server Room in support of Law Enforcement Authorities in fighting terrorism, organised crime and cybercrime (encryption)
	Biometric identification techniques and systems for criminal identification; a European biometric assessment centre	<ul style="list-style-type: none"> Automatic Fingerprint Identification System (AFIS) implementation, SIS revision (face recognition and tattoo image content retrieval systems) Fingermarks in Schengen Information System (SIS)
Link to other activities (incl. cross-reference, integration and laboratories)	CS transversality to security topics (hybrid threats, critical infrastructure protection, border management, anticipation and technology assessment)	<ul style="list-style-type: none"> Trust chains in issuing identity and travel documents, softID and traditional documents Sensor technologies in construction sector (buildings & infrastructures) Smart-Borders: Schengen Master List operational system (digital certificates for electronic passport authentication); mobile apps for ETIAS (European Travel Information & Authorisation System) Laissez Passer CS landscape (hybrid threats) Application for EEAS (CoOL, Consular OnLine) for information exchange and cooperation in major crises Internet Topology Portal
Cooperation	Cyber threats. NATO/EU	

Source: Authors.

3.4.6 Chemical, biological, radiological, nuclear and high-yield explosive threats

The JRC is very active regarding nuclear safeguards using technologies and tools for nuclear material measurements and standards, containment and surveillance, as well as process monitoring. In particular, the JRC supports the Illicit Trafficking Radiation Assessment Program ⁽²⁷⁴⁾, which evaluates the performance of available commercial radiation detection equipment against consensus standards. The JRC also implements hands-on training and testing schemes for the detection of radionuclide materials (via the European Nuclear Security Training Centre) ⁽²⁷⁵⁾ and plays a role in following up on incidents involving the seizure of nuclear material. The JRC can determine the origin of nuclear materials for forensics purposes and brings this expertise to Member States. All these activities ensure that nuclear material is not diverted from peaceful use.

The JRC coordinates ERNCIP ⁽²⁷⁶⁾, a framework for sharing knowledge and expertise for better protection of critical infrastructures against all types of hazards, including CBRN-E threats. The JRC offers its know-how to improve management of industrial chemical risks and the implementation of the Seveso Directive-Technological Disaster Risk Reduction, as well as evaluating atmospheric dispersion models. It also works on the detection of homemade explosives and the protection of airports.

The JRC is involved in the standardisation of biological toxin measurements as well as the harmonisation of biological threat detection equipment. It contributes to the proper implementation of dual-use export control policies through guidelines, technical advice and training, with a special focus on tangible-intangible transfers, transit, trans-shipment and brokering. Finally, the JRC offers technical support to the EU CBRN CoE, the main objective of which is to strengthen the institutional capacity of partner countries in order to mitigate CBRN risks.

It is also worth noting that the JRC carried out a CBRN-E landscape study in 2017 (McCourt et al., 2017) and has edited in collaboration with Europol a CBRN-E glossary ⁽²⁷⁷⁾ to foster a common understanding of key terms.

Figure 35 provides more a detailed overview of the JRC's work in the area of CBRN-E, organised by topic, action and deliverable.

⁽²⁷⁴⁾ European Commission, 'Illicit Trafficking Radiation Assessment Program (ITRAP+10) test campaign summary report' (<https://ec.europa.eu/jrc/en/publication/illicit-trafficking-radiation-assessment-program-itrap10-test-campaign-summary-report>).

⁽²⁷⁵⁾ European Commission, 'The European Nuclear Security Training Centre (EUSECTRA)' (<https://ec.europa.eu/jrc/en/european-nuclear-security-training-centre-eusectra>).

⁽²⁷⁶⁾ European Commission, 'European Reference Network for Critical Infrastructure Protection (Erncip)' (<https://ec.europa.eu/jrc/en/network-bureau/european-reference-network-critical-infrastructure-protection-erncip>). See also Section 2.2.

⁽²⁷⁷⁾ European Commission, 'Welcome to the European CBRNE Glossary' (<http://opencbrne.jrc.ec.europa.eu/main>).

Figure 35: Overview of JRC actions and deliverables in the area of CBRN-E, 2018

topics	actions	deliverables
Expansion, enhancement, development and consolidation of the CBRN-E activity	Strategy for a coherent handling of CBRN-E activities across JRC, seizing the opportunity to establish Knowledge Centres (CBRN-E and dual trade)	<ul style="list-style-type: none"> • Support for harmonised implementation of chemical & biological (CB) threat security policies. Enhance capabilities in CB risk mitigation by following up actions endorsed by the EU MS in their CBRN Action Plan • Development of Community of Practice for Strategic Trade Control
	Execution of landscape/knowledge mapping and analysis of stakeholders, interoperability and harmonisation, emergency preparedness and risk assessment, dual use and export control	<ul style="list-style-type: none"> • Collection of strategic trade control related best-practices, guidelines and open source wires
	Foster capabilities in the field of chemical & biological (CB) threats at international level and within the EU	<ul style="list-style-type: none"> • Studies on current portable devices and on assessment of new B portable detection equipment. Compilation of published guidelines for standard measurement procedure performance requirements of B threat agent detection devices • Device for detection of pathogen agents for security application • Research on explosives and chemical substances, and appraisal of detection equipment and testing methodologies for priority applications • Standards for performance assessment of RN detection and measurement equipment. Contribution to international standards (ISO/IEC) for performance tests of equipment used against CBRN threats. EUFRAT programme to participate in pre-normative research and tests of equipment and draft standards • European programme for the establishment of validated procedures for the detection and identification of biological toxins. Certified reference materials for the threat biotoxins
	Definition and implementation of a strategy on CBRN-E risk management at international level	<ul style="list-style-type: none"> • Creation of a network of trainers and training institutes used in the CBRN CoE initiative • Support to project cycle and CoE network. Mapping of trainings, compilation of training materials, development of a CoE training programme. Maintenance of the CoE Open Source Centre • Support to the EU Export control outreach programme; The current phase is the EU Long Term Programme (LTP) on export control • NAQ (Needs Assessment Questionnaire) support to the CoE Partner Countries. Support to the development of CBRN National Action Plans (NAPs) by the partner countries' authorities
	Building up partnership and CBRN-E capacity building within and across borders of the MS	<ul style="list-style-type: none"> • Training activities for licensing/customs officers
	Sendai framework for disaster risk reduction as a tool for the promotion of results. Cotonou partnership agreement to foster the objectives of the CBRN CoE	<ul style="list-style-type: none"> • Scientific & technical support for harmonised implementation of B threat security policies • ERNCIP (European Reference Network for Critical Infrastructure Protection) groups on CBRNE will deliver pre-norms, technical specifications and workshop agreements to CEN/ CENELEC (European Committee for Standardization)
	Studies on existing and developing patterns of resilience throughout society, depending on i.a. social and economic context	<ul style="list-style-type: none"> • Context specific risk perception and resilience patterns for individuals and their inter-dependency relationships with society (families, communities, authorities)
	Further development of the JRC competences on data mining, text mining, tracing financial flows and smuggling flows	<ul style="list-style-type: none"> • Provision of expertise related to the list of dual-use items and emerging technologies of concern. Collects and analyse key data in support of EU export control policy. Review information concerning violations, prosecution cases, illicit transactions and geopolitical issues
	Support EU export control policy, especially the harmonised implementation of dual-use items' export control policies	
	Extend the CBRN-E training platform (training modules on risk assessment and disaster risk management)	<ul style="list-style-type: none"> • Using Dir E's Blackboard Learning Management System (LMS), creation of e-courses, specifically a Needs Assessment Questionnaire to National Action Plan e-course to be used to fulfil various training needs • Training activities under the CBRN CoE initiative
	European programme for the establishment of validated procedures for the detection and identification of biological toxins	<ul style="list-style-type: none"> • The EuroBioTox core members will develop and validate improved analytical tools, reagents and standard operating procedures. Training courses will be developed and attended by the EuroBioTox network partners

Source: Authors.

3.4.7 Hybrid threats

In order to support the implementation of Action 5 specified in the joint communication on countering hybrid threats, the JRC recently produced vulnerability and detection indicators, which were presented to the EU Member States in December 2017 (Giannopoulos et al., 2018).

By mid-2018, the JRC had set up a transversal project on hybrid threats (Hybrit), which started in 2019, based on the consideration that no one alone can tackle research on this topic, owing to its unprecedented complexity, which requires something other than traditional defence mechanisms. Therefore, cross-sectoral and cross-actor information exchange is needed within a multidisciplinary approach, involving areas in which the JRC is already active, such as cybersecurity, critical infrastructure protection, media analysis (text mining and fake news), resilience, big data, and disaster and risk management. This project will consist of several work packages addressing the most challenging needs, notably the development of a conceptual framework on hybrid threats, and the area of early detection of hybrid threats.

Furthermore, the JRC and Hybrid CoE have been jointly developing a conceptual framework to characterise and better understand hybrid threats (see Section 2.7.2 for details).

Figure 36 provides more a detailed overview of the JRC's work in the area of hybrid threats, organised by topic, action and deliverable.

Figure 36: Overview of JRC actions and deliverables in the area of hybrid threats, 2018

topics	actions	deliverables
Critical and hybrid risks and key vulnerabilities	Vulnerability & Risk assessment of critical energy infrastructure	<ul style="list-style-type: none"> Development of indicator framework to assess resilience of critical energy infrastructure
Monitoring non-military components of hybrid threats	Social media disinformation	<ul style="list-style-type: none"> Media Monitoring and Open Source Information Analysis against disinformation. Detection and handling of disinformation ("fake news") Monitoring and analysis of social media
Situational awareness by composition of different streams of information and analysis	Further integration of social media monitoring into existing tools	<ul style="list-style-type: none"> Operational support to STAR (Strategic analysis and response capability). Support, maintain and update the EMM Installation for EEAS Europol Media Monitoring. Enhance Europol's capabilities in preventing and combating organised crime, terrorism and other forms of serious crime Court of Justice Media Monitor
Resilience strategies for countering hybrid threats strategies	Develop specific hybrid risk related indicators for critical infrastructure and supply chains	<ul style="list-style-type: none"> Main focus will be on gas transmission networks and power transmission grids
	Development of vulnerability indicators for hybrid threats	<ul style="list-style-type: none"> Assess their vulnerabilities with respect to Hybrid Threats
	Situational awareness tools and risk assessment methodologies for hybrid threats	<ul style="list-style-type: none"> Probabilistic approach to assess resilience of critical energy infrastructure. Assess resilience by combining risk assessment and reliability analysis methods
	Guidance for MS to apply indicators and self-assess the level of their vulnerability	<ul style="list-style-type: none"> Provide MS with a set of vulnerability indicators and methodological elements to assess their vulnerabilities with respect to Hybrid Threats

Source: Authors.

3.4.8 Space

The greater part of the JRC's space activities is devoted to Earth observation, including scientific research and operations linked to the Copernicus Global Land and Emergency Services, and support for environmental monitoring, climate change, agriculture (i.e. the common agricultural policy) and food security, the bioeconomy, water resources, renewable energies, transport, development cooperation, disaster and emergency management, marine and maritime issues, global and border security, and migration. There is also notable expertise in the JRC on GNSS (Galileo and EGNOS), radiofrequency spectrum, wireless communications (emerging 5G), protection of critical infrastructures and space weather. The JRC collaborates with space industry actors, Member State space agencies, EUMETSAT, the ESA, SatCen and the GSA. Worldwide, it works with the Group on Earth Observation and the G8 Committee on Earth Observing Satellites as well as the UN (the Office for Outer Space Affairs, the International Maritime Organization, the Food and Agriculture Organisation, the World Food Programme and the International Committee on Global Navigation Satellite Systems). Furthermore, the JRC is also active in other areas that are critically related to space, notably geospatial data infrastructures, the digital single market, cybersecurity, resilience, and security and defence.

Figure 37 provides more a detailed overview of the JRC's work in the area of space, organised by topic, action and deliverable.

Figure 37: Overview of JRC actions and deliverables in the area of space, 2018

topics	actions	deliverables
Partnership with DG GROW on the future of the Copernicus and Galileo flagships	Contribution to mid-term review of the Copernicus Emergency Management Service (EMS)	• Report on the Copernicus EMS Mapping service including a summary on the main achievements, service developments, as well as international cooperation
	Support to defining the evolution of COPERNICUS	• Management and new developments for the Copernicus flood EWS
	Support to the market uptake of governmental positioning, navigation and timing services of Galileo	• In the near future, the development of precise chip-scale devices for timing and inertial navigation will reach a cost-effective trade-off, sufficient for a wide commercial exploitation. The JRC will investigate potential issues and needs for legislative intervention on the exploitation of these new navigation and positioning devices including new techniques for the integration with satellite data
	Support the definition of the evolutions of the GNSS programmes (Galileo 2nd, EGNOS v3)	• Co-organizing the ESA/JRC summer school on GNSS in 2018 and 2019 • Survey on new commercial devices exploiting modern physics concepts and their reliability with respect to GNSS navigation • On DG GROW request, the JRC will monitor the progress and review an H2020 project developing an ionospheric prediction service (IPS). Validation of the forecasting products delivered by the project prior to its planned deployment at the Galileo Service Center
	Facilitate testing and demonstration activities under R&D actions of the EU GNSS programmes	• Position resilience using GNSS. Development of a demonstrator able to effectively integrate different data types from GNSS, inertial and opportunistic sources • Maintenance and operation of a network of ionospheric scintillation stations in sites located in the Equatorial Region and in Antarctica • Operation, maintenance and upgrade of JRC's GNSS testing facilities: they are currently being made accessible to third parties including: Project Consortia running R&D Projects under the EU GNSS Programmes and GNSS receiver/antenna manufacturers • Support to the European GNSS Agency (GSA) in different areas like: Galileo user segment operational readiness, H2020 and Galileo Fundamental Elements, Galileo Security and PRS (User Segment development, Pilot Projects definition and implementation), Galileo and EGNOS Exploitation (Service provision, system evolution, cooperation with other GNSS) • Support to Galileo Service Validation. JRC will support the GSA Exploitation Department in the context of Service Validation activities, addressing Signal-In-Space performance • Performing of an extensive testing campaign on eCall modules, including a verification of the technical requirements for compatibility of eCall in-vehicle systems with the positioning services provided by the Galileo and EGNOS systems. In a second phase the testing setup will be defined, including the receivers under test, the constellation simulator and Labview scripts • Performing of a testing campaign targeting Maritime navigation and radio communication equipment, including Global navigation satellite systems (GNSS) receivers, and Galileo in particular • Under the support to EU GNSS Programmes, permanent monitoring of the performance of Galileo and other GNSS. • Support to GROW in the context of the Galileo Compatibility, Signals and Interoperability Working Group (CSI WG); and also in the framework of negotiations with GNSS and non-GNSS providers on the compatibility between Galileo and other systems • Following the declaration of Early services in 2017, a new milestone is planned for Galileo to increase its commitment in terms of user performance. JRC will carry out measurements and performance analysis first to shape the new commitment targets and second to verify that the commitments are kept. New figures of merit will be defined and verified, including Position Dilution of Precision and Position Accuracy
Radio-frequency	Radio-frequency spectrum management - tested for 5G communication; applications as Mobile Broadband, Public Safety communication, Smart Cities, Intelligent Transport System; Special band for emergency services	• Support to the initiatives led by DG GROW towards the establishment of the first EU Radio Navigation Plan. The expected market uptake of Galileo will depend on the future of present radionavigation infrastructures and the entrance of new players. A radio navigation plan should map this new scene and becomes instrumental when setting the strategy of the EU GNSS Programmes. JRC will contribute to this mapping exercise
JRC strategy approach to space	Co-ordination structure for Space activities as part of its KM approach	• Set up and management of the CoP on Space; participation to inter-service group on space
	New support areas dedicated to: EU as global actor; emerging EEAS requirements; Commission defence initiatives (especially dual use aspects defence-civil security); support to EC and EEAS roles in CEOS, GEOS and other international bodies	
	Scientific support to EC/EEAS policy makers, INTCEM and Agency operational users in a KM approach, i.e. integrating outside JRC knowledge and forward looking, related to the use of space assets	• Space & security landscape study. It will concern the intersection of space and security: use of space for security, and security of space-related infrastructure. • Report on the JRC expertise and on the state of the art of EU-funded civil security research, that have relevance to potential future EU defence research • Report on Horizon scanning on space, security and migration.
	Application of high flying technology and near space missions. Study on the integration of commercial space assets with government owned space assets	• Near-Space High-Altitude Platforms (NS-HAD) pre-exploratory research activity
	Security of space assets and related infrastructure; includes space situational awareness (SSA), space weather; links to radio spectrum, critical infrastructure protection and cybersecurity; space supply chain	• Support to the policy initiatives towards the implementation of the Space Strategy adopted in October 2016. In particular, JRC will contribute to the review of the evaluation and impact assessment studies of the GovSatCom and SST programmes

Source: Authors.

4 Future avenues for security and defence research and development

In this chapter the authors suggest directions for developments in the security and defence R&D, by building block (Section 4.1). This future oriented discussion is complemented by more specific foresight insights gathered from a topical horizon scanning exercise carried out at the Joint Research Centre (Section 4.2).

4.1 Subject-specific developments

4.1.1 Border control

Among possible future areas for R & D in border control, the following can be mentioned.

Data management. With the implementation of the Entry–Exit System and ETIAS, in addition to all the other systems such as VIS, SIS, Eurodac, PNR and advance passenger information, the amount of data to be collected, stored, analysed and exchanged will grow exponentially. Robust R & D activities in data analysis will be necessary to support national security by enabling more accurate screening against watch lists or creating risk profiles that allow authorities to identify where to deploy resources and where to target their interventions.

Biometric technology. Facial recognition is now being widely used in various applications to verify identity. However, identity fraud remains a key area of weakness for border management. More work needs to be done on properly matching names and faces. There is also a very large amount of research needed to improve efficiency in the use of biometric technology (e.g. biometric on the move solutions) to create a seamless, smart and sustainable experience for travellers while ensuring the highest possible level of security.

Monitoring and surveillance. The integrity of physical borders remains critical, particularly in areas with long land or sea borders. Their surveillance can be enhanced by using technological innovations in both sensors (infrared sensors, heat-sensing cameras and various types of radar) and platforms (satellite and unmanned vehicles), as well as in the areas of sensor data integration and analysis and of system interoperability for information exchange.

Standardisation and interoperability. The technical specifications of the equipment used by border guards are frequently provided and tested by the vendors alone. There is no reliable information that can be used to assess technical strengths and weaknesses in relation to performance results. No clear EU certification exists for this equipment. In addition, how interoperable the equipment is is not always known.

4.1.2 Critical infrastructure protection

Given the number of initiatives and the wealth of knowledge that has been produced in this domain, any future work should focus mainly on connecting the dots and establishing communities that can help to improve the resilience of critical infrastructures. The knowledge centres established by the European Commission can be considered a best practice in this regard and be applied to other areas.

This, however, does not exclude conducting research on new or emerging issues affecting the protection and resilience of critical infrastructures. Research should be adapted on the basis of the evolution of critical infrastructures in the next 5 years, as described in Section 2.2.4, in order to provide the necessary knowledge.

In particular, it is expected that more research on AI and machine learning will be needed to address two major upcoming challenges. The first is the tendency to have more autonomous systems that require intelligent algorithms embedded within machine-learning capabilities. This revolution is already taking place in the transport sector, in particular in road transport, and it is expected to grow. The second main challenge is the large amount of data produced by infrastructures as a result of increased connectedness and ICT pervasiveness (e.g. smart systems); these data need to be analysed to adapt the performance of critical infrastructures and render their services more efficient.

Research should also take into account to a greater extent the needs of the defence sector and accommodate them to provide reassurance that future critical infrastructures will be able to take on board defence-related needs. Increasing concerns about hybrid threats and the need for closer collaboration between the civilian and defence sectors will result in a blurring of the limits between the two domains even in the context of research.

4.1.3 Public space protection

Terrorist organisations are continuously innovating in their techniques and modus operandi. Therefore, the EU needs to be equally innovative in its response, harnessing technology and pooling expertise to detect and counter or mitigate emerging threats (Karlos et al., 2018b), notably drones and ramming vehicles.

Drones can easily overcome ground-based protective perimeters and efficiently deliver explosives (Larcher et al., 2017), weapons or harmful substances, or conduct reconnaissance to prepare for a ground attack. Work is ongoing (European Aviation Safety Agency, 2017) to introduce regulations to ensure the safety and security of civilian-operated drones ⁽²⁷⁸⁾.

Commercial drones constitute a problem also for the military. American forces during the Mosul siege faced ISIS attacks with small drones dropping grenades and miniaturised explosives. Clearly, this is a classical case leading to a search for dual-use solutions. The great challenges are first the detection of these small drones and then the identification of suitable countermeasures for their neutralisation.

To detect small drones, different types of sensors and technologies can be used, such as radar, acoustic, thermal, laser and radio-magnetic (Tarchi et al., 2014). Some are passive — they use the radio, acoustic or thermal emission of the intruding object to detect it — while others are active and base their detection on the reflection of a signal generated by the sensor when it hits the drone. Difficulties arise from the facts that existing radar systems are designed to detect much bigger objects and that most drones are constructed of plastic (not easily spotted electronically), are small and fly low to the ground.

With regard to countermeasures, various solutions are employed: communication jamming, GPS jamming, GPS spoofing, drone engine jamming, wind-blowing machines, water cannons, shooting and net-trapping systems delivered by guns or other drones. These countermeasures should lead to the development of two ways of combating terrorist drones (Fitzpatrick, 2018): 'hard kill' solutions that involve physically disabling drones and 'soft kill' ones that bring them down electronically.

Regarding the use of vehicles as weapons, this is not expected to cease and shows that critical infrastructures are no longer the main target of terrorists, as this would require substantial resources and extensive planning, with the chances of success being low. However, an increase in vehicle-ramming attacks is expected, as they are easily planned and require minimal expertise, and a variety of vehicles can be accessed without difficulty. In response to this threat, several countries are trying to introduce physical security measures that aim to make crowded places safe. However, these measures are not always selected based on a structured approach; rather, selection largely depends on the practices adopted by the local security authorities and the availability of specific solutions. There is clearly a growing need to design and implement specialised methods and techniques to increase the safety of public spaces (Karlos et al., 2017). Moving from a one-size-fits-all to a tailor-made approach would require the development of a European standard for barrier testing (European Committee for Standardization, 2010) and the introduction of a simple and clear barrier selection procedure that can be used by security officers, premises owners, building designers, technical experts and other interested professionals. In the EU, documentation on the design, installation methodologies, cost and selection of available products is rather limited, and encouragement and effort on the part of the European Commission towards the development of such material would be useful.

Protection can also be achieved through the concept of smart cities, which includes the deployment of sensors for various applications in the urban environment. These sensors can also be used to increase the safety of public spaces. They build complex systems and need specific measurements and analysis approaches to provide metrics for performance assessment. Novel metrics and analysis methods (e.g. agent-based modelling, graph theory, machine learning) can set the basis for the integration of intelligent streaming of sensor data and distributed signal processing into large-scale networks for the realisation of smart and safe cities.

New detection technologies have recently been developed that allow monitoring of a much greater flow of people. This could enable a much more flexible use in many situations where nowadays detection is simply not possible (e.g. in transport hubs and shopping malls). However, more detection also implies more alarms, both false and accurate. For busy public spaces, this means getting prepared both in terms of training and reaction capacities.

Because of the open nature of our society, new public space protection measures will always be characterised and triggered by emerging threats. Therefore, it is difficult to identify needs for further protection.

⁽²⁷⁸⁾ European Commission, draft regulation laying down rules and procedures for the operation of unmanned aircraft, Brussels.

Incorporating safety measures into the design of buildings and public spaces will always be useful. The need for detection will also continue to be very high, as new dangerous materials will need to be identifiable. These includes new home-made explosives, highly toxic substances and weapons built by 3D printers.

4.1.4 Critical supplies security

Technologies are becoming more and more complex, achieving more sophisticated effects and finding novel applications. Some of these technologies — AI, big data analytics, robotics, new energy systems, additive manufacturing, advanced and smart materials, quantum computing, virtual and augmented reality, unmanned systems, remote sensing — enable products to produce new effects and therefore are central to most modern civil and military (dual-use) applications.

R & D in relation to materials is at the heart of some of these technologies. It is also seen as a priority for innovation and a source of competitive advantage. Much of the ongoing research on materials involves investigating their structure and properties at a very small scale. For instance, currently there is a great deal of competition worldwide to translate the potential of materials such as graphene into real applications. An example of an innovation success story is the development of carbon fibre, which has become recognised as a strong, resilient and lightweight composite material. This material is a feasible substitute for heavier steel and aluminium in many industrial applications including in aerospace, automotives, energy, construction and sporting equipment.

The energy transition has produced an important collateral effect in the replacement of energy-intensive technologies and products with products and technological processes using raw materials (new minerals and critical metals) intensively. The current increase in demand in the world and the EU for critical raw materials and other minerals and metals (including those considered to be base metals by now) is unsustainable, and the security of their responsible and sustainable sourcing is becoming a real challenge, reflected in recent policy documents and media reporting. The notion of 'trade wars' has been mentioned frequently in the past 2 years by actors in global political and societal movements. The EU is creating its own responses to these threats, such as actions to promote endogenous EU industrial value chains for strategic products using raw materials intensively (e.g. batteries) and actions relating to the end-of-life of products and raw material supply chains (e.g. recycling, reuse).

4.1.5 Cybersecurity

Demand for EU policies related to cybersecurity, privacy, data protection and cybercrime is clearly here to stay and will most probably increase over the coming years, with the aims of better protecting the rights of individuals, ensuring national security, developing new EU digital infrastructures and services, and further developing EU industry and the EU economy.

From an R & D perspective, areas that will need support include the following:

- With the general data protection regulation now in force in the EU, work will be needed to better specify the technical requirements imposed by the new legislation.
- Cybersecurity and privacy will have to be further streamlined in all traditional industrial sectors benefiting from the ICT revolution, such as energy, transport, finance, health and nuclear power.
- Law enforcement actors and judicial communities will need to combat effectively with new tools, procedures and cooperation schemes the increasing challenge posed by the use of ICT in terrorism, organised crime and cybercrime.
- Internal security will have to rely on more integrated EU large-scale IT systems (fuelled by national and central databases containing more reliable and accurate information), as well as on more trustworthy identity and travel documents (less prone to fraudulent manipulation, required for all individuals and with a convergence of security measures imposed on non-EU nationals and EU citizens).
- The defence and external security dimension of cybersecurity — including hybrid threats emerging from cyberspace, dual use of some ICT and export control issues — will call for an increase in synergies and bridges between the civil and military worlds.
- The socioeconomic dimensions of cybersecurity will require more attention from both policymakers and researchers in the social sciences. On the one hand, the economy of cybersecurity, the costs of cybercrimes, the risks that digital technologies entail and the associated liabilities will have to be further addressed. On the other hand, societal aspects, including, in particular, awareness raising, digital hygiene,

education, ethics and cyber professional skills, may require new policy initiatives. Behavioural insights could also be applied to understand such societal aspects.

4.1.6 Chemical, biological, radiological, nuclear and high-yield explosive threats

To combat CBRN-E threats, R & D should focus on surveillance but also on preparedness and response, especially for first responders.

A better understanding of possible future CBRN-E attacks should be developed, for example of which products/materials could be used, alone or in combination (based on ease of access and ease of manipulation, hazard, potential dissemination, public vulnerabilities, etc.). Innovative methods for early detection of CBRN-E threats (sensors, with wide spectrum), suitable for use by first responders or for automatic use, are much needed. Automatic CBRN-E sensors (alone or in series) can be used in public spaces for constant monitoring and early warning systems. Studies on the appropriate combination of such sensors with air-flow modelling in closed or semi-open public spaces are required to protect public spaces and critical infrastructures. The creation of specific measurements, including standards and certification for detection equipment, are needed for a greater comparability of data detection, both within EU and beyond. A specific project accomplishing this task is the ITRAP project (described in Section 3.4.6).

Concerning response, research should aim to improve the protective equipment used by first responders, facilitate its use and reduce the costs. The communication and IT tools used during this type of intervention should be improved. Tools for quick and efficient triage of victims need to be upgraded. Light but protective equipment for front-line healthcare personnel in hospitals is required. The development of appropriate medical countermeasures and availability plans will necessitate further reflection and adaptation. Decontamination methods are a central topic because they are often very expensive and time-consuming; new products and technologies are required.

Finally, in the face of a CBRN-E incident, the whole of society is affected; police, military, government and healthcare services must be qualified and coordinated before an incident occurs. Methods for continuous cooperation between relevant actors should be developed and exercises organised on a regular basis in the EU.

4.1.7 Hybrid threats

The issue of hybrid threats has not been yet adequately addressed by the research community, which can be attributed to a lack of awareness, especially before the events in Ukraine. Taking into account the lead time between the identification of a research need and its actual implementation in terms of project proposals and execution of the work, it should not be a surprise that outcomes from the scientific community are still rather limited. However, this situation is changing and more institutions are aiming to carry out work in the domain of hybrid threats.

There are specific challenges related to attribution of hybrid threats, which seems to be one of the most demanding issues in the domain. It is expected that significant research will be required on data fusion, visual analytics and related techniques, to develop methods and tools that will support security authorities in correlating data from different sources. Such work could contribute to situational awareness, early warning and attribution of hybrid threats.

The volume of data will probably continue to increase in the years to come and as a consequence new methods based on AI should emerge. This area of research should be at the core of future efforts towards data fusion to facilitate attribution.

Given the nature of hybrid threats, more research is needed to gain a better understanding of the interactions between technological systems and societies. Such research should focus on identifying the emerging behaviour of complex sociotechnical systems.

Tackling hybrid threats is certainly an issue that will benefit from dual-use research, considering that this topic is by definition a dual-use concept, since it is tightly linked to hybrid warfare. Although hybrid warfare and hybrid threats are not the same issue, they are closely related and it is expected that research addressing the challenges posed by each of them will ultimately help in tackling both.

4.1.8 Combating radicalisation

Regarding digital technology and social media used for radicalisation, there is a need to make people less vulnerable and more resilient to such profiling.

According to the Radicalisation Awareness Network (2016), the following are the main research needs:

- to better identify the causes, processes and mechanisms of radicalisation in order to develop effective preventive measures and countermeasures;
- to understand the relationships between radicalisation, violent extremism and terrorism;
- to grasp how visual and audio materials influence individuals on their radicalisation path;
- to better connect measures aimed at combating and preventing radicalisation with insights we have gained into how radicalisation functions in the first place;
- to overcome the false exceptionalism of radicalisation;
- to compare different types of radicalisation based on different ideologies;
- to change the current structure of research funding needs.

Political scientist Gøtzsche-Astrup (2018) calls for a focus on research designs capable of arbitrating on matters of causality, not just correlation. He argues that because both theoretical approaches and current interventions propose cause-and-effect relationships, it is imperative that research shifts its focus to experimental research designs capable of making causal inferences. With the help of empirical evidence, we could increase our knowledge to gain a better understanding radicalisation mechanisms by mapping which interventions work effectively.

4.1.9 Fighting against terrorism financing

According to a study commissioned by the European Parliament's Policy Department for Citizens' Rights and Constitutional Affairs (European Parliament, 2018b), mitigating the terrorism financing risks associated with virtual currencies is a significant security priority. Although these risks are currently a low priority owing to the limited number of publicly documented and confirmed cases, there is a need to pursue and better understand developments in this technology, as its use could increase significantly in the future because of its high levels of privacy and anonymity.

Another appealing feature for terrorists that might lead them to adopt virtual currencies more broadly is the utilisation of encryption technology on social media and other online platforms. In addition, a better understanding of the nexus between terrorist actors and other criminal activities (e.g. between terrorism with cybercrime) would make it possible to better identify where to focus efforts to design resilient solutions to anticipate terrorism financing through virtual currencies.

Furthermore, because of the trend towards lower cost terrorist attacks, there is a need to better understand possible scenarios and monitor potential target areas to prepare communities for and make them resilient to such events.

4.1.10 Space

The recent JRC landscape study on space and security (Lagazio et al., 2019) reviewed space- and security-related R & D projects funded either at EU level or at national level in eight countries (Belgium, Germany, Spain, France, Italy, Norway, Sweden and the United Kingdom). This study also analysed several capability gaps. This was done by comparing EU policies and strategies with existing capabilities. By combining this analysis with a survey of current R & D efforts, it identified several as yet insufficiently addressed areas that need (further) research:

- cybersecurity for space infrastructures;
- the physical protection and resilience of space-related assets;
- the development and evolution of space-enabled resources and services specifically for users in the security domain, including for emerging users such as law enforcement;
- advanced secure satellite communication (SATCOM).

These topics should benefit from EU-level R & D funding, for example under the new framework programme Horizon Europe or the EDF.

Furthermore, the following priorities were listed:

- promote and support big data research infrastructures for space, to fully exploit all space data collected and the potential for combining them with non-space big data;
- include SSA systems and their development as a structural element of the European space R & D landscape, aiming at a global SSA system of systems, and develop SST to deal with increasing pressure from orbital congestion and deep space needs;
- promote security-by-design approaches to R & D for space infrastructures, to facilitate affordable solutions that are better aligned with security requirements;
- extend the coverage of Copernicus and Galileo/EGNOS, and provide a long-term R & D vision for their development, taking into account the security user communities' needs;
- develop virtual R & D initiatives for security domains of strategic importance, involving end users and manufacturers as well as the research community;
- support the development of spin-off mechanisms from space-related R & D so that key European security domains benefit more from space developments.

4.2 Horizon scanning on security

In the context of its foresight activities ⁽²⁷⁹⁾, the JRC organised in 2018 a horizon-scanning exercise focusing on security. This is a foresight method for identifying emerging issues that may be of future importance in the context of security. The main results of this exercise are presented hereafter, following a brief account of the methodology used.

4.2.1 Methodology

JRC staff were invited to submit items — factual information from research studies, articles, news items, conference presentations, blogs, social media posts, etc. — about developments indicating something new, different and potentially important in the domain of security. The items submitted were then discussed in a 'sense making' session, the purpose of which was to detect new trends, drivers of change, weak signals or discontinuities. Based on the discussion of 120 items relating to recent events or situations, the participants in the sense-making session identified over 70 individual issues, which were then clustered into 26 common issues. These issues were then mapped by the participants, according to their perceived importance for security and the extent to which they were already addressed within the JRC. The mapping was followed by a prioritisation exercise, where each participant was allowed to express one positive vote (for an issue that merited further consideration in the JRC in the context of security consequences) and one negative vote (for an issues that did not need further consideration either because it was already addressed by the JRC or because it was considered of less importance for the JRC and the EU in terms of security consequences).

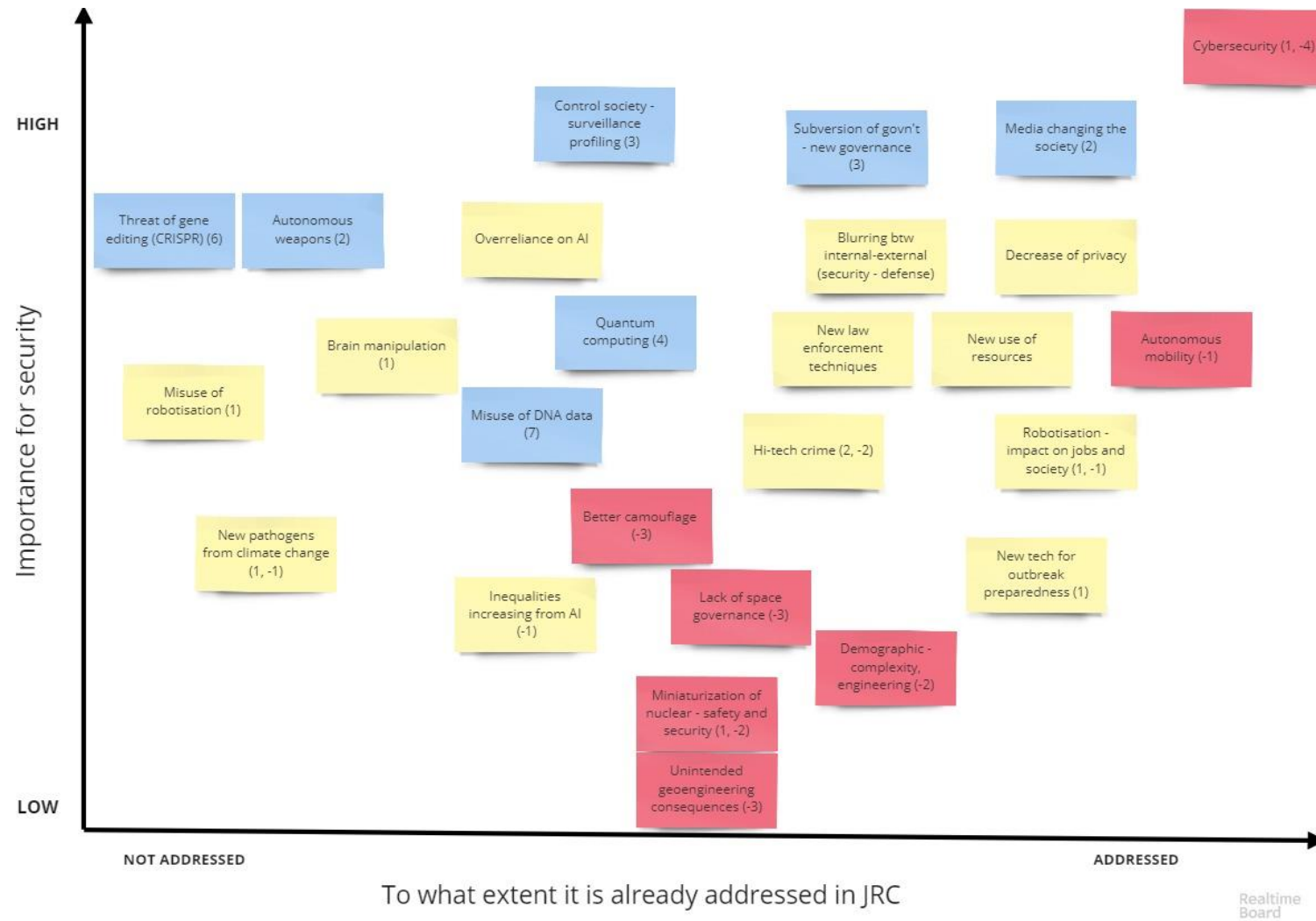
4.2.2 Results

The results of the mapping and prioritisation of the 26 issues are depicted in **Figure 38**.

The mapping positions the security issues along the horizontal axis (extent to which they are addressed by the JRC at the time of the exercise) and the vertical axis (participants' perceived importance for security). The prioritisation (i.e. whether the issue merits further consideration in the JRC in the context of security consequences or not) is depicted using colour coding. Issues presented on blue labels are those that received two or more positive votes; those on pink ones got two or more negative votes; yellow labels indicate issues that obtained one or zero votes, or an equal number of positive and negative votes. The number in brackets indicates the number of votes received.

⁽²⁷⁹⁾ European Commission, 'Foresight and horizon scanning' (<https://ec.europa.eu/jrc/en/research/crosscutting-activities/foresight>).

Figure 38: Horizon scanning mapping and prioritisation



Source: Authors.

4.2.2.1 Issues considered important and not (or not to a significant extent) addressed by the JRC

The top left quadrant in **Figure 38** includes eight issues that participants concluded were most important for security and not or not adequately addressed, at the time of the exercise, by JRC. They are presented hereafter, in decreasing order of votes ⁽²⁸⁰⁾.

The first two issues received the highest number of positive votes, indicating that a high proportion of the participants in the workshop considered them issues that needed to be addressed.

Misuse of DNA data. With affordable and faster genome sequencing technologies, more and more DNA data is becoming available, stored in private and public databases. This data holds important personal information and, with the use of machine-learning algorithms, there are ways of de-anonymising it.

— Main topical security aspects: privacy, ethical dimensions, cybersecurity.

— *Main overarching discipline: life sciences, data.*

Threat of gene editing (CRISPR). The wide availability and low cost of gene editing technologies brings the danger of engineering pathogens that could be used as bioweapons, and also the possibility of engineering human embryos.

— Main topical security aspects: (bio)terrorism, CBRN-E, ethical dimensions, hybrid threats.

— *Main overarching discipline: life sciences.*

Quantum computing. The creation of quantum computers will increase the processing capacities and computing power. More immediately, it will impact cryptography and cybersecurity in general. However, increased computing power and communication speed means increased speed of online interactions, sensing, positioning etc.

— Main topical security aspects: cybersecurity, cryptography.

— *Main overarching discipline: physics/technology* ⁽²⁸¹⁾.

Control society — surveillance profiling. Increased connectivity and availability of big data regarding economic and social interactions allow for closer monitoring of the behaviour of individuals. This can infringe the right to privacy and enable interventions in society on this basis (such as China's social rating system).

— Main topical security aspects: privacy, ethical dimensions.

— *Main overarching discipline: life sciences, data.*

Autonomous weapons. The development of AI and robotics will enable the creation of autonomous weapons that could change the nature of warfare and the landscape of threats.

— Main topical security aspects: terrorism, defence, hybrid threats, cybersecurity.

— *Main overarching discipline: technology.*

Brain manipulation. While currently privacy concerns relate to people's physical or online activities, there are increased attempts to impact brain activity (e.g. interpreting and manipulating brain activity, direct brain simulation).

— Main topical security aspects: privacy, ethical dimensions.

— *Main overarching discipline: life sciences.*

Misuse of robotisation. Autonomous devices (robots, drones) will feature more prominently in people's everyday lives. While they can have many positive roles, the safety and security aspects are considerable. On the other hand, autonomous security robots can be used for unmanned patrolling, surveillance and inspection.

— Main topical security aspects: terrorism, defence, cybersecurity.

— *Main overarching discipline: technology.*

⁽²⁸⁰⁾ The main security topical aspects and main overarching disciplines are deduced from the selected items which inspired the clustering of issues (see Annex 7).

⁽²⁸¹⁾ In these analyses and comments, "technology" includes all developments related to artificial intelligence.

Note: this issue is strongly linked to the abovementioned autonomous weapons, as they have many aspects in common.

Overreliance on AI ⁽²⁸²⁾. Increased dependence on algorithms running different processes leaves people vulnerable to wrong decisions taken by AI systems, as the machine-learning methods applied reproduce biases or do not sufficiently interpret the context of a given situation.

— Main topical security aspects: privacy, ethical dimensions.

— *Main overarching discipline: technology.*

4.2.2.2 Issues considered important and already addressed by the JRC

The top right quadrant of **Figure 38** gathers the 10 issues that participants considered as being important and already addressed within the JRC. The votes for the first two issues indicate that they need to be addressed further:

Subversion of government — new governance. The reliance on central government for the provision of public goods has been waning with increased decentralisation and individualisation. People are experimenting with governance approaches for large-scale cooperation between the people without the coordination of a central authority.

— Main topical security aspects: privacy, blockchains, ethical dimensions.

— *Main overarching discipline: social sciences.*

Media changing the society. Social media have changed the society in the social (relationships, identity), economic (personal brands, advertising, online micro transactions) and political (echo-chambers, fake news psychometrics) spheres, which have an impact on the perceptions and understanding of security.

— Main topical security aspects: social media, terrorism, privacy, ethical dimensions.

— *Main overarching discipline: social sciences.*

High-tech crime. Technology is reshaping governance of crime organisation (e.g. crime-as-a-service) and creating new opportunities in cybercrime, but also new approaches to organising police work (e.g. crowdsourcing).

— Main topical security aspects: organised crime, cybersecurity, law enforcement.

— *Main overarching discipline: technology.*

Robotisation — impact on society. The trend for replacing current jobs with AI and robots will require a different organisation of society, which could lead to tensions and upheavals.

— Main topical security aspects: ethical dimensions.

— *Main overarching discipline: social sciences.*

Blurring the line between security and defence. With increased digital activity and globalisation, the strict division between external defence issues and internal security issues is no longer possible in the face of hybrid threats.

— Main topical security aspects: terrorism, cybersecurity, hybrid threats, defence.

— *Main overarching discipline: technology.*

Decreased privacy. Increased use of data in various spheres of life (health, consumption, mobility) means that people have been increasingly sacrificing their privacy for the convenience of better products and services or for security.

— Main topical security aspects: privacy, ethical dimensions, cybersecurity.

— *Main overarching discipline: data.*

⁽²⁸²⁾ Since this horizon scanning exercise, the JRC planned a set of deliverables on these aspects for 2019/2020.

New law enforcement techniques. New technologies have an impact on law enforcement techniques, especially regarding image processing, mobile tracking, etc.

— Main topical security aspects: privacy, ethical dimensions, law enforcement.

— *Main overarching discipline: technology.*

New use of resources. The scarcity of resources will lead to increased tensions; new technologies with new security concerns are emerging (e.g. small modular nuclear reactors); and resources will play an important role in any consideration of space exploration.

— Main topical security aspects: supply of (critical) raw materials, organised crime.

— *Main overarching discipline: technology.*

Two issues received a negative priority rating (i.e. no need for further consideration): **cybersecurity** (since it is already widely addressed within the JRC and the Commission) and **autonomous mobility**.

4.2.2.3 Issues considered of less importance for security

Finally, eight issues were considered by participants to have relatively few security implications. Only three had one positive vote: 'New pathogens from climate change', 'New tech for outbreak preparedness' and 'Inequalities increasing from AI'. The remaining five received a negative rating: 'Miniaturisation of nuclear reactors', 'Unintended geoengineering consequences', 'Lack of space governance', 'Better camouflage' and 'Demographics — complexity, engineering'.

Table 9 gathers the issues considered by participants most important in terms of security concerns, and their main overarching discipline, deduced from the selected items that inspired the clustering of issues (see Annex 7).

Table 9: Horizon scanning: security issues by main overarching discipline

Issues		Life sciences	Physics/technology	Data	Social sciences
Misuse of DNA data	<i>Issues considered important and not (or not to a significant extent) addressed by the JRC</i>	X		X	
Threat of gene editing		X			
Quantum computing			X		
Control society — surveillance profiling		X		X	
Autonomous weapons			X		
Brain manipulation		X			
Misuse of robotisation			X		
Overreliance on AI			X		
Subversion of government — new governance	<i>Issues considered important and already addressed by the JRC</i>				X
Media changing the society					X
High-tech crime			X		
Robotisation — impact on society					X
Blurring the line between security and defence			X		
Decreased privacy				X	
New law enforcement techniques			X		
New use of resources			X		

Source: Authors.

Table 10 gathers the issues considered by participants most important in terms of security concerns and their main topical aspects, deduced from the selected items that inspired the clustering of issues (see Annex 7).

Table 10: Horizon scanning: security issues by main topical aspects

Issues	Terrorism	Cybersecurity	Organised crime	Defence	Privacy	Cryptography	CBRN-E	Ethical dimensions	Social media	Hybrid threats	Law enforcement	Supply of raw materials	Block chains
Not (or not to a significant extent) addressed by the JRC													
Misuse of DNA data		X			X			X					
Threat of gene editing	X						X	X		X			
Quantum computing		X				X							
Control society — surveillance profiling					X			X					
Autonomous weapons	X	X		X						X			
Brain manipulation					X			X					
Misuse of robotisation	X	X		X						X			
Overreliance on AI					X			X					

Issues	Terrorism	Cybersecurity	Organised crime	Defence	Privacy	Cryptography	CBRN-E	Ethical dimensions	Social media	Hybrid threats	Law enforcement	Supply of raw materials	Block chains
Addressed by the JRC													
Subversion of government — new governance					X			X					X
Media changing the society	X				X			X	X				
High-tech crime		X	X								X		
Blurring the line between security and defence	X	X		X						X			
Decrease of privacy		X			X			X					
New law enforcement techniques					X			X			X		
Robotisation — impact on society								X					
New use of resources			X									X	
Total	5	7	2	3	8	1	1	10	1	4	2	1	1

Source: Authors.

4.2.3 Comments

With regard to the main overarching discipline (**Table 9**), half of the issues fall under the heading 'physics/technology' (including AI), which is not surprising, as issues relating to AI, robots, unmanned systems, etc. are very numerous. In addition, physics/technology issues are equally distributed between those already addressed by the JRC and those not yet or not sufficiently addressed.

Maybe a more significant forward-looking observation is the relative importance of issues relating to life sciences. They represent one quarter of the issues (4 out of 16), but even more worthy of note is that they all belong to the group of issues that are not yet addressed by the JRC (4 out of 8). And the two issues with the largest numbers of votes are life sciences ones. This may indicate a trend that will need to be monitored with increased care: the growing role of manipulation of the living, raising all kinds of concerns, including with regard to security.

This can be seen also in the topical aspects that characterise these security issues (**Table 10**): concerns about privacy and ethical dimensions (each relating to more than half of the issues) are the major topics by far that emerge from this analysis.

More focused horizon-scanning sessions might allow fine-tuning of these first conclusions.

5 Conclusions

The aim of this study was to provide in a single document a landscape review of security and defence R & D in the EU. For this purpose, a substantive part of the report has been dedicated to setting the scene, that is, describing current security threats, policy initiatives and strategies in place for combating them, the main stakeholders involved (including the specific contributions of the JRC) and the relevant legislation in the field. This overview has been carried out with a focus on various building blocks (i.e. thematic areas).

The backstage picture has been completed with a history of the EU security and defence R & D programmes and funding. Against this background, 349 thematically relevant R & D projects financed from 2014 to 2018 under the H2020 framework programme were identified and analysed on the basis of several criteria.

Among the results obtained from the analysis of these projects, two are worth highlighting here. First, despite the fact that about one third of the projects are multi-thematic (i.e. linked to two or more building blocks), there is a very uneven thematic project distribution: whereas half of the projects deal with various cybersecurity aspects, several blocks, such as hybrid threats or countering terrorism financing, have a very low number of projects. There is obviously potential for more thematically balanced project selection in the future. Second, the overwhelming majority (90 %) of the projects were characterised as having potential dual-use applications, meaning that their outputs with civil application could also be used in the defence sector. More fine-tuned analysis is however needed on this important aspect.

Finally, suggestions for future avenues for security and defence research have been made for each building block specifically, and, furthermore, the results of a foresight exercise carried out in the JRC hint at the importance of life sciences for the future and the attention that will need to be paid to the growing role of manipulation of the living, which raises all kinds of concerns, including in terms of security.

This 2019 edition of this landscape report is meant to be the basis for an online living document, to be updated with new data and analysis when appropriate. A potential avenue for future enrichment would be an analysis of EU-funded R & D projects in terms of achieved outputs and impact on society at large (e.g. innovation, policy development, knowledge transfer and dissemination, etc.), once the H2020 framework programme is completed. Another area for future deeper analysis is the dual-use potential of such projects. This last analysis being undertaken by the editorial team for this report and should be available early in 2020.

Bibliography

References

Ahmed, M., and Lloyd George, F., *A War of Keywords: How extremists are exploiting the internet and what to do about it*, Tony Blair Institute for Global Change, London.

Alarid, M. (2016), 'Recruitment and radicalization: the role of social media and new technology', in Hughes, M., and Miklaucic, M. (eds.), *Impunity: Countering illicit power in war and transition*, Center for Complex Operations, Institute for National Strategic Studies, National Defence University, Washington DC, pp. 313-329.

Aliu, M., Bektashi, M., Sahiti, A., and Sahiti, A. (2017), 'A review of sources on terrorist financing', *Acta Universitatis Danubius. Juridica*, Vol. 13, No 1, pp. 97-108.

Andersson, J. J., and Tardy, T. (2015), 'Hybrid: what's in a name?', European Union Institute for Security Studies Brief, Issue 32.

Atran, S. (2016), 'The devoted actor: unconditional commitment and intractable conflict across cultures', *Current Anthropology*, Vol. 57, S13, pp. 192-203.

Bailes, A. J. K. (2005), 'The European security strategy: an evolutionary history', SIPRI Policy Paper No 10, Stockholm International Peace Research Institute, Stockholm.

Bloemkolk, I. C. (2015), 'The European fight against the financing of terrorism', bachelor's thesis, University of Twente, Department of Public Administration.

Bordin, G., Flore, M., Hristova, M., Luque-Perez, E., Nazareth, C., Piccinini, P., Ruzzante, G., and Tartaglia, G. (2017), *Cybersecurity Landscape Study*, European Commission, Brussels and Ispra.

Borum, R. (2014), 'Psychological vulnerabilities and propensities for involvement in violent extremism', *Behavioral Sciences and the Law*, Vol. 32, No 3, pp. 286-305.

Brattberg, E., and Maurer, T. (2018), 'Russian election interference: Europe's counter to fake news and cyber attacks', Carnegie Endowment for International Peace, Washington DC.

Canadian Security Intelligence Service (2018), *Who Said What? The security challenges of modern disinformation*, World Watch: Expert Notes, Canadian Security Intelligence Service, Ottawa.

Carus, W. S. (2017), 'A short history of biological warfare: from pre-history to the 21st century', Center for the Study of Weapons of Mass Destruction Occasional Paper, No 12, National Defense University Press, Washington DC.

Cassara, J., and Jorisch, A. (2010), 'Gold and Diamonds' (Chapter 6), in *On the Trail of Terror Finance: What law enforcement and intelligence officers need to know*, Red Cell Intelligence Group, Washington DC.

Centre for Strategy and Evaluation Services (2011a), Ex-post evaluation of preparatory action on security research (PASR) and interim evaluation of FP7 security research: Final report, Centre for Strategy and Evaluation Services, Sevenoaks, United Kingdom.

Centre for Strategy and Evaluation Services (2011b), *Final evaluation of the competitiveness and innovation framework programme: Final report*, Centre for Strategy and Evaluation Services, Sevenoaks, United Kingdom.

Clunan, A. L. (2013), 'The fight against terrorist financing', *Political Science Quarterly*, Vol. 121, No 4, pp. 569-596.

Council of the European Union (2005a), *The European Union Counter-Terrorism Strategy* (14469/4/05), Brussels.

Council of the European Union (2005b), *The EU strategy for combating radicalisation and recruitment to terrorism* (14781/1/05), Brussels.

Council of the European Union (2008), *Revised EU strategy for combating radicalisation and recruitment to terrorism* (15175/08), Brussels.

Council of the European Union (2010), *Internal Security Strategy for the European Union: Towards a European security model*, Luxembourg, Publications Office of the European Union.

Council of the European Union (2014a), *European Union Maritime Security Strategy (EUMSS) — Action plan* (17002/14), Brussels.

Council of the European Union (2014b), *EU Cyber Defence Policy Framework* (15585/14), Brussels.

Council of the European Union (2014c), Revised EU strategy for combating radicalisation and recruitment to terrorism (9956/14), Brussels.

Council of the European Union (2014d), Draft guidelines for the EU strategy for combating radicalisation and recruitment to terrorism (13469/1/14), Brussels.

Council of the European Union (2015), Draft Council conclusions on the renewed European Union internal security strategy 2015-2020 (9798/15), Brussels.

Council of the European Union (2017a), Annual report on the implementation of the cyber defence policy framework (15870/17), Brussels.

Council of the European Union (2017b), Review of the guidelines for the EU strategy for combating radicalisation and recruitment to terrorism (6700/17), Brussels.

Council of the European Union (2017c), Resolution of the Council and of the Representatives of the Governments of the Member States, meeting within the Council, on the European Union Work Plan for Sport (1 July 2017-31 December 2020) (9639/17), Brussels.

Council of the European Union and Council of the European Space Agency (2010), 7th Space Council Resolution, 'Global challenges: taking full benefit of European space systems', Brussels, 25 November 2010.

Dengg, A., and Schurian, M. (eds.) (2006), *Networked Insecurity: Hybrid threats in the 21st century*, National Defence Academy, Institute for Peace Support and Conflict Management, Vienna.

Dewar, R. S. (2017), *Active Cyber Defense*, CSS Cyber Defense Trend Analysis, Center for Security Studies, ETH Zürich.

EDA (European Defence Agency) (2016), 'Factsheet on preparatory action on CSDP-related research', 27 October 2016.

EDA (2017a), 'Protection of critical energy infrastructure: conceptual paper', EDA, PCEI expert group, Brussels.

EDA (2017b), Consultation Forum for Sustainable Energy in the Defence and Security Sector (CF SEDSS): Final report by the European Defence Agency to the European Commission: Directorate-General Energy.

EEAS (European External Action Service) (2016), 'Shared vision, common action: a stronger Europe — a global strategy for the European Union's foreign and security policy', EEAS, Brussels.

EEAS, 2018, 'A Europe that protects: countering hybrid threats', EEAS, Brussels.

Eeten, M., van, Nieuwenhuijs, A., Luijff, E., Klaver, M., and Cruz, E. (2011), 'The state and the threat of cascading failure across critical infrastructures: the implications of empirical evidence from media incident reports', *Public Administration*, Vol. 89, No 2, pp. 381-400.

ENISA (European Union Agency for Cybersecurity) (2017), *ENISA Programming Document 2018-2020*.

ESRIF (European Security Research and Innovation Forum) (2009), *ESRIF Final Report*.

EUISS (European Union Institute for Security Studies) (2016), European Defence Research: The case for an EU-funded defence R & T programme — Report of the Group of Personalities on the preparatory action for CSDP-related research, EUISS, Paris.

Eurojust (2017), *Eurojust CBRN-E Handbook*, Version VI.

European Aviation Safety Agency (2017), Notice of Proposed Amendment 2017-05 (A): Introduction of a regulatory framework for the operation of drones — Unmanned aircraft system operations in the open and specific category, European Aviation Safety Agency, Cologne.

European Commission (2004), *Research for a Secure Europe: Report of the Group of Personalities in the field of security research*, Office for Official Publications of the European Communities, Luxembourg.

European Commission (2006), Meeting the Challenge: The European security research agenda — A report from the European Security Research Advisory Board, Office for Official Publications of the European Communities, Luxembourg.

European Commission (2013a), *CIP Performance Report* (available at http://ec.europa.eu/cip/files/cip/cip-performance-report-october-2013_en.pdf).

European Commission (2013b), 'Factsheet: Horizon 2020 budget'.

European Commission (2015), Final evaluation of security research under the seventh framework programme for research, technological development and demonstration: Final report — Executive summary, Publications Office of the European Union, Luxembourg.

European Commission (2016a), Strategic Plan 2016-2020 of DG Migration and Home Affairs.

European Commission (2016b), Strategic Plan 2016-2020 of DG Internal Market, Industry, Entrepreneurship and SMEs.

European Commission (2016c), Strategic Plan 2016-2020 of DG International Cooperation and Development.

European Commission (2016d), Strategic Plan 2016-2020 of DG Mobility and Transport.

European Commission (2016e), Strategic Plan 2016-2020 of DG Regional and Urban Policy.

European Commission (2016f), Strategic Plan 2016-2020 of DG Energy.

European Commission (2016g), Strategic Plan 2016-2020 of DG Environment.

European Commission (2016h), Strategic Plan 2016-2020 of DG Trade.

European Commission (2017a), *Study on the review of the list of critical raw materials: Criticality assessments*, Directorate-General for Internal Market, Industry, Entrepreneurship and SMEs, Brussels doi:10.2873/876644.

European Commission (2017b), Annual Activity Report of DG Energy.

European Commission (2017c), *Security Research and Innovation: Boosting the effectiveness of the security union*, Publications Office of the European Union, Luxembourg.

European Commission (2018), Management Plan of DG Migration and Home Affairs.

European Commission (2019), 'Security union: a Europe that protects', (available at https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/european-agenda-security/20190320_agenda-on-security-factsheet-progress-report_en.pdf)

European Committee for Standardization (2010), *Vehicle Security Barriers: Performance requirements, test methods and guidance on application* (CWA16221), European Committee for Standardization, Brussels.

European Council (2003), *European Security Strategy: A secure Europe in a better world*, Brussels.

European Court of Auditors (2014), *The External Borders Fund has fostered financial solidarity but requires better measurement of results and needs to provide further EU added value* (Special Report No 15/2014), Publications Office of the European Union, Luxembourg.

European Parliament (2015a), *At a Glance: Understanding hybrid threats*, European Parliamentary Research Service, Brussels.

European Parliament (2015b), *NGOs and Money Laundering: Adapting EU rules to engage NGOs better*, European Parliamentary Research Service, Brussels.

European Parliament (2016a), *The Future of EU Defence Research*, Brussels.

European Parliament (2016b), *At a Glance: Preparatory action on defence research*, European Parliamentary Research Service, Brussels.

European Parliament (2017), *Countering Terrorist Narratives*, Brussels.

European Parliament (2018a), *The Fight against Terrorism: Cost of non-Europe report*, European Parliamentary Research Service, Brussels.

European Parliament (2018b), *Virtual Currencies and Terrorist Financing: Assessing the risks and evaluating responses*, European Parliament, Policy Department for Citizens' Rights and Constitutional Affairs, Brussels.

European Union (2008), *Report on the implementation of the European security strategy: Providing security in a changing world* (Report S407/08), Brussels.

Europol (2017), *European Union Terrorism Situation and Trend Report 2017*, Europol, The Hague.

Europol (2018a), *Europol Programming Document 2018-2020*, Europol, The Hague.

- Europol (2018b), European Union Terrorism Situation and Trend Report 2018, Europol, The Hague.
- FATF (Financial Action Task Force) (2008), *Terrorist financing*, FATF, Paris.
- FATF (2012), International standards on combatting money laundering and the financing of terrorism & proliferation: The FATF recommendations (updated October 2016), FATF, Paris.
- FATF (2015a), Emerging Terrorist Financing Risks, FATF, Paris.
- FATF (2015b), Financing of the terrorist organisation Islamic State in Iraq and the Levant (ISIL), FATF, Paris.
- Fitzpatrick, A. (2018), 'TIME special report: the drone age', *TIME Magazine*, 11 June 2018.
- Francis, R., and Bekera, B. (2014), 'A metric and frameworks for resilience analysis of engineered and infrastructure systems', *Reliability Engineering and System Safety*, Vol. 121, pp. 90-103.
- Freeman, M. (2011), 'The sources of terrorist financing: theory and typology', *Studies in Conflict and Terrorism*, Vol. 34, pp. 461-475.
- Freeman, M., and Ruehsen, M. (2013), 'Terrorism financing methods: an overview', *Perspectives on Terrorism*, Vol. 7, No 4, pp. 5-26.
- Gattinesi, P. (2018), *European Reference Network for Critical Infrastructure Protection: ERNCIP Handbook 2018 edition*, Publications Office of the European Union, Luxembourg, doi:10.2760/245080.
- Gerwehr, S., and Daly, S. (2006), 'Al-Qaida: terrorist selection and recruitment', in Kamien, D., *McGraw-Hill Homeland Security Handbook*, McGraw-Hill Companies, pp. 73-89.
- Giannopoulos, G., Theocharidou, M., Theodoridis, G., and Gattinesi, P. (2018), *Developing Vulnerability and Detection Indicators for Hybrid Threats*.
- Giannopoulos, G., Smith, H., and Theocharidou, M. (2019), *The Landscape of Hybrid Threats: A conceptual model*, JRC (forthcoming).
- de Goede, M., and Wesseling, M. (2017), 'Secrecy and security in transatlantic terrorism finance tracking', *Journal of European Integration*, Vol. 39, No 3, pp. 253-269.
- Gøtzsche-Astrup, O. (2018), 'The time for causal designs: review and evaluation of empirical support for mechanisms of political radicalisation', *Aggression and Violent Behavior*, Vol. 39, pp. 90-99.
- GSA (European Global Navigation Satellite Systems Agency) (2017), *GNSS Market Report*, Issue 5.
- Hariharan, A. (2012), 'Hawala's charm: what banks can learn from informal funds transfer systems', *William and Mary Business Law Review*, Vol. 3, No 1 pp. 273-308.
- High-Level Expert Group on Radicalisation (2018), *Final Report*.
- High Representative of the Union for Foreign Affairs and Security Policy (2016), *Implementation Plan on Security and Defence* (14392/16), Brussels, 14 November 2016.
- Hoffman, F. (2014), 'On not-so-new warfare: political warfare vs hybrid threats', War on the Rocks (<https://warontherocks.com/2014/07/on-not-so-new-warfare-political-warfare-vs-hybrid-threats/>).
- Hogg, M. A., and Adelman, J. (2013), 'Uncertainty-identity theory: extreme groups, radical behavior, and authoritarian leadership', *Journal of Social Issues*, Vol. 69, No 3, pp. 436-454.
- Institute for Economics and Peace (2017), Global Terrorism Index 2017: Measuring and understanding the impact of terrorism, Report 55.
- Jost, P. M., and Sandhu, H. S. (2000), *The hawala alternative remittance system and its role in money laundering*, United States Department of the Treasury, Financial Crimes Enforcement Network (FinCEN) and Interpol/FOPAC.
- Kalvach, Z., et al. (2016), *Basics of Soft Targets Protection: Guidelines*, Soft Targets Protection Institute, Prague.
- Karlos, V., and Larcher, M. (2018), *Workshop on the Protection of Public Spaces*, European Commission, JRC114223.
- Karlos, V., Larcher, M., and Solomos, G. (2017), *Review on Vehicle Barrier Protection Guidance*, JRC Science for Policy Report, Publications Office of the European Union, Luxembourg, doi:10.2760/845599.

- Karlos, V., Larcher, M., and Solomos, G. (2018a), Guideline: Selecting proper security barrier solutions for public space protection — Protection against vehicle-ramming attacks, JRC113778.
- Karlos, V., Larcher, M., and Solomos, G. (2018b), *Review on Soft Target / Public Space Protection Guidance*, JRC Science for Policy report, Publications Office of the European Union, Luxembourg, doi:10.2760/553545.
- Keneally, M., and Madden, P. (2017), 'Concerts, other soft targets remain vulnerable to attack, experts say', ABC News (<https://abcnews.go.com/US/concerts-soft-targets-remain-vulnerable-attack-experts/story?id=47582876>).
- Koehler, D. (2016), *Understanding Deradicalization: Methods, tools and programmes for countering violent extremism*, Routledge, New York.
- Kumari, A., and Sharma, A. K. (2017), 'Infrastructure financing and development: a bibliometric review', *International Journal of Critical Infrastructure Protection*, Vol. 16, pp. 49-65.
- Lagazio, M., Alves dos Santos, H., Pillon, E., and Greidanus, H. (2019), *Landscape Study on Space and Security: Policies, stakeholders, capabilities and R & D in Europe*, Publications Office of the European Union, Luxembourg.
- Larcher, M., Karlos, V., Valsamos, G., and Solomos, G. (2017), *Scenario Study: Drones carrying explosives*, JRC107683 (limited dissemination).
- Luijff, E., Nieuwenhuijs, A., Klaver, M., van Eeten, M., and Cruz, E. (2010), 'Empirical findings on European critical infrastructure dependencies', *International Journal of System of Systems Engineering*, Vol. 2, No 1, pp. 3-18.
- Matrix Insight (2008), *Study to assess the extent of abuse of non-profit organisations for financial criminal purposes at EU level*, commissioned by the European Commission's Directorate-General for Justice, Freedom and Security.
- McCauley, C., and Moskaleiko, S. (2017), 'Understanding political radicalization: the two-pyramids model', *American Psychologist*, Vol. 72, No 3, pp. 205-216.
- McCourt, J., Greidanus, H., Lequarré, A. S., Tartaglia, G. P., Abousahl, S., Goulart, M., Clark, I., Gattinesi, P., Krausmann, E., Wood, M., Nordvik, J. P., Larcher, M., Pinto, A., Anderson, D., Meersman, B., Florian, D., Trapmann, S., Zeleny, R., Van den Eede, G., Berthou, V., Janssens, W., Luetzenkirchen, K., and Sevini, F. (2017), *CBRNE Landscape Study*, European Commission, Geel, Brussels, Ispra and Karlsruhe.
- McGregor, I., Hayes, J., and Prentice, M. (2015), 'Motivation for aggressive religious radicalization: goal regulation theory and a personality × threat × affordance hypothesis', *Frontiers in Psychology*, Vol. 6, p. 1325.
- Miller, C., and Selig Chauhan, L., (2017), 'Radical beliefs and violent behaviour', in Colaert, L. (ed.), *'De-radicalisation': Scientific insights for policy*, Flemish Peace Institute, Brussels, pp. 23-45.
- Miller, J., and Gerth, J. (2001) 'A nation challenged: Al Qaeda; honey trade said to provide funds and cover to bin Laden', New York Times (available at <https://www.nytimes.com/2001/10/11/world/nation-challenged-al-qaeda-honey-trade-said-provide-funds-cover-bin-laden.html>).
- Money Laundering and Threat Assessment Working Group (2005), *US Money Laundering Threat Assessment*.
- Nai-Fovino, I., Neisse, R., Lazari, A., Ruzzante, G., Polemi, N., and Figwer, M. (2018a), *European Cybersecurity Centres of Expertise Map: Definitions and taxonomy*, Publications Office of the European Union, Luxembourg.
- Nai-Fovino, I., Neisse, R., Lazari, A., and Ruzzante, G. (2018b), *European Cybersecurity Centre of Expertise: Cybersecurity competence survey*, Publications Office of the European Union, Luxembourg.
- Nan, C., Sansavini, G., and Kröger, W. (2016), 'Building an integrated metric for quantifying the resilience of interdependent infrastructure systems', in Panayiotou, C. G., Ellinas, G., Kyriakides, E., and Polycarpou, M. M. (eds.), *Critical Information Infrastructures Security, 9th International Conference on Critical Information Infrastructures Security, CRITIS 2014: Revised selected papers*, Springer International Publishing, pp. 159-171.
- Napoleoni, L. (2005), 'Terrorism financing in Europe', *Journal of Middle Eastern Geopolitics*, Vol. 1, No 2, pp. 47-58.
- NATO Energy Security Centre of Excellence (2017), *Hybrid Threats: Overcoming ambiguity, building resilience*, NATO Energy Security Centre of Excellence, Vilnius.

Neumann, P. R. (2017), Countering violent extremism and radicalisation that lead to terrorism: Ideas, recommendations, and good practices from the OSCE region, International Centre for the Study of Radicalisation, King's College London.

NIS Cooperation Group (2019), Sectorial implementation of the NIS Directive in the Energy sector, Report - CG Publication 03/2019.

Oftedal, E. (2015), *The Financing of Jihadi Terrorist Cells in Europe*, Norwegian Defence Research Establishment, Kjeller.

Osborn, P. (2017), 'Cyber border security: defining and defending a national cyber border', *Homeland Security Affairs* 13, Article 5 (available at <https://www.hsaj.org/articles/14093>).

Ouyang, M., Dueñas-Osorio, L., and Min, X. (2012), 'A three-stage resilience analysis framework for urban infrastructure systems', *Structural Safety*, Vol. 36-37, pp. 23-31.

Passas, N. (2003), Informal Value Transfer Systems, Terrorism and Money Laundering, US Department of Justice, Washington DC.

Pavel, C., and Tzimas, E. (2016), *Raw materials in the European Defence Industry*, European Commission, Joint Research Centre, Luxembourg.

Pellerin C. (2016), 'Communicating terror: an analysis of ISIS communication strategy', Kuwait programme, Paris Institute of Political Studies, Paris.

Picarelli, J. T. (2009), 'The future of terrorism', *NIJ Journal*, Vol. 264, pp. 26-30.

Radicalisation Awareness Network (2016), 'Radicalisation research: gap analysis', RAN Research Paper.

Radicalisation Awareness Network (2017), Preventing Radicalisation to Terrorism and Violent Extremism: Approaches and practices.

Ranlet, P. (2000), 'The British, the Indians, and smallpox: What actually happened at Fort Pitt in 1763?', *Pennsylvania History*, Vol. 67, No 3, pp. 427-441.

Rieger, D., Frischlich, L., and Bente, G. (2013), *Propaganda 2.0: Psychological effects of right-wing and Islamic extremist internet videos*, Wolters Kluwer Deutschland GmbH, Cologne.

Roy, O. (2016), *The Global Appeal of the Islamic State*, Hurst and Company, London.

Ruehsen, M. (2001), 'Foreign trade detected as refuge for launderers dodging tougher laws', *Money Laundering Alert*.

Scalia, T., Di Mezza, A., Masini, A., Sylvestre, S., Thomas, R., Szabo, J.-L., De Heide, M., Butter, M., and Parker, D. (2017), *Study on the dual-use potential of key enabling technologies (KETs): Final technical report*, Contract No EASME/COSME/2014/019.

Schmid A. P. (2013), Radicalisation, De-Radicalisation, Counter-Radicalisation: A conceptual discussion and literature review, ICCT Research Paper, International Centre for Counter-Terrorism, The Hague.

Setola, R., and Theocharidou, M. (2016), 'Modelling dependencies between critical infrastructures', in Setola, R., Rosato, V., Kyriakides, E., and Rome, E. (eds.), *Managing the Complexity of Critical Infrastructures: Studies in systems, decision and control*, Vol. 90. Springer International Publishing, Cham, pp. 19-41.

Setola, R., Luijff, E., and Theocharidou, M. (2016), 'Critical infrastructures, protection and resilience', in Setola, R., Rosato, V., Kyriakides, E., and Rome, E. (eds.), *Managing the Complexity of Critical Infrastructures: Studies in systems, decision and control*, Vol. 90, Springer International Publishing, Cham, pp. 1-18.

Styczinski, J., Beach-Westmoreland, N., and Stables, S. (2016), When the Lights Went Out: A comprehensive reviews on the 2015 attacks on the Ukrainian critical infrastructure, Booz Allen Hamilton.

Tarchi, D., Mias, S., Oliveri, F., Baldini, G., Sanchez, I., Fortuny, J., Borio, D., Larcher, M., and Solomos, G. (2014), *Drones Overflight of Nuclear Power Plants: Can IPSC help?* JRC Technical Report (limited distribution).

Thoma, K. (ed.) (2011), *European Perspectives on Security Research*, Springer-Verlag, Berlin and Heidelberg.

Tofangsaz, H. (2018), 'Criminalization of terrorist financing: from theory to practice', *New Criminal Law Review*, Vol. 21, No 1, pp. 57-140.

Treverton, G., Thvedt, A., Chen, A., Lee, K., and McCue, M. (2018), *Addressing Hybrid Threats*, European Centre of Excellence for Countering Hybrid Threats and Swedish Defence University.

UN (United Nations) (1996), United Nations General Assembly Resolution A/RES/51/210, 88th Plenary Meeting, 17 December 1996.

UN (1999), International Convention for the Suppression of the Financing of Terrorism, 54/109, 9 December 1999.

UN Office for Outer Space Affairs (2017), *International Space Law: United Nations instruments*, United Nations, Vienna.

UN Security Council (2004), Resolution 1540, adopted on 28 April 2004.

UN Security Council (2015), Resolution 2250, adopted on 9 December 2015.

UNDP (United Nations Development Programme) (2016), Preventing violent extremism through promoting inclusive development, tolerance and respect for diversity (revised 2017), UNDP, New York.

UNODC (United Nations Office on Drugs and Crime) (2016), Handbook on the management of violent extremist prisoners and the prevention of radicalization to violence in prisons, Criminal Justice Handbook Series, United Nations, Vienna.

USDOS (United States Department of State) (2005), *International Narcotics Control Strategy Report, Volume II: Money laundering and financial crimes*, Bureau for International Narcotics and Law Enforcement Affairs, Washington DC.

Webber, D., and Kruglanski, A. W. (2018), 'The social psychological makings of a terrorist', *Current Opinion in Psychology*, Vol. 19, pp. 131-134.

Wesseling, M. (2013), 'The European fight against terrorism financing: professional fields and new governing practices', PhD thesis, University of Amsterdam, Faculty of Social and Behavioural Sciences.

WHO (World Health Organization) (2007), International Health Regulations (2005): Areas of work for implementation, WHO, Geneva.

World Economic Forum (2014), The Future Availability of Natural Resources: A new paradigm for global resource availability, World Scenario Series.

Zdanowicz, J. (2009), 'Trade-based money laundering and terrorist financing', *Review of Law and Economics*, Vol. 5, No 2, pp. 855-878.

Legislation and policy documents from the European Union institutions

Council of the European Union

Council of the European Union, Common Military List of the European Union adopted by the Council on 9 February 2015 (equipment covered by Council common position 2008/944/CFSP defining common rules governing the control of exports of military technology and equipment), OJ C 129, 21 April 2015.

Council of the European Union, Council common position on combating terrorism (2001/930/CFSP), Brussels, 27 December 2001.

Council of the European Union, Council common position updating common position 2001/931/CFSP on the application of specific measures to combat terrorism and repealing common position 2009/67/CFSP (2009/468/CFSP), Luxembourg, 15 June 2009.

Council of the European Union, Council conclusions, revised Presidency conclusions of the European Council of 14 December 2007 (16616/1/07), Brussels, 14 February 2008.

Council of the European Union, Council conclusions on a strategic framework for European cooperation in education and training ('ET 2020') (2009/C 119/02), Brussels, 12 May 2009.

Council of the European Union, Council conclusions on common security and defence policy (15992/13), Brussels, 25 November 2013.

Council of the European Union, Council conclusions partly on common security and defence policy (EUCO 217/13), Brussels, 20 December 2013.

Council of the European Union, Council conclusions EUCO 79/14, Brussels, 27 June 2014.

Council of the European Union, Council conclusions on development of a renewed European Union internal security strategy, Brussels, 4 December 2014.

Council of the European Union, Council conclusions EUCO 11/15, Brussels, 20 March 2015.

Council of the European Union, Council conclusions on energy diplomacy (10995/15), Brussels, 20 July 2015.

Council of the European Union, Council conclusions on a framework for a joint EU diplomatic response to malicious cyber activities ('Cyber Diplomacy Toolbox') (9916/17), Brussels, 7 June 2017.

Council of the European Union, Council conclusions on the joint communication to the European Parliament and the Council: Resilience, deterrence and defence: Building strong cybersecurity for the EU (14435/17), Brussels, 20 November 2017.

Council Decision 2002/630/JHA of 22 July 2002 establishing a framework programme on police and judicial cooperation in criminal matters (AGIS), OJ L 203, 1.8.2002, p. 5-8.

Council Decision 2007/124/EC, Euratom, of 12 February 2007 establishing for the period 2007 to 2013, as part of General Programme on Security and Safeguarding Liberties, the Specific Programme 'Prevention, Preparedness and Consequence Management of Terrorism and other Security-related risks', OJ L 58, 24.2.2007, p. 1-6.

Council Decision 2007/125/JHA of 12 February 2007 establishing for the period 2007-2013, as part of the General Programme on Security and Safeguarding Liberties, the Specific Programme 'Prevention of and Fight against Crime', OJ L 58, 24.2.2007, p. 7-12.

Council Decision 2013/743/EU of 3 December 2013 establishing the specific programme implementing Horizon 2020 — the Framework Programme for Research and Innovation (2014-2020) and repealing Decisions 2006/971/EC, 2006/972/EC, 2006/973/EC, 2006/974/EC and 2006/975/EC, OJ L 347, 20.12.2013, p. 965-1041.

Council Decision 2014/75/CFSP of 10 February 2014 on the European Union Institute for Security Studies, OJ L 41, 12.2.2014, p. 13-17.

Council Decision 2014/401/CFSP of 26 June 2014 on the European Union Satellite Centre and repealing Joint Action 2001/555/CFSP on the establishment of a European Union Satellite Centre, OJ L 188, 27.6.2014, p. 73-84.

Council Decision (CFSP) 2015/203 of 9 February 2015 in support of the Union proposal for an international Code of Conduct for outer-space activities as a contribution to transparency and confidence-building measures in outer-space activities, OJ L 33, 10.2.2015, p. 38-44.

Council Decision (CFSP) 2018/340 of 6 March 2018 establishing the list of projects to be developed under PESCO, OJ L 65, 8.3.2018, p. 24-27.

Council Decision (CFSP) 2018/1797 of 19 November 2018 amending and updating Decision (CFSP) 2018/340 establishing the list of projects to be developed under PESCO, OJ L 294, 21.11.2018, p. 18-22.

Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection, OJ L 345, 23.12.2008, p. 75-82.

Council Directive 2009/119/EC of 14 September 2009 imposing an obligation on Member States to maintain minimum stocks of crude oil and/or petroleum products, OJ L 265, 9.10.2009, p. 9-23.

Council Regulation (EC) No 428/2009 of 5 May 2009 setting up a Community regime for the control of exports, transfer, brokering and transit of dual-use items, OJ L 134, 29.5.2009, p. 1-269.

Council Resolution of 26 September 2008, 'Taking forward the European Space Policy', OJ C 268, 23.10.2008, p. 1-6.

European Commission

European Commission, Commission communication, 'European defence: industrial and market issues — towards an EU defence equipment policy' (COM(2003) 113), Brussels, 11 March 2003.

European Commission, Commission communication, 'Implementation of the preparatory action on the enhancement of the European industrial potential in the field of security research: towards a programme to advance European security through research and technology' (COM(2004) 72 final), Brussels, 3 February 2004.

European Commission, Commission communication, 'Security research: the next steps' (COM(2004) 590 final), Brussels, 7 September 2004.

European Commission, Commission communication, 'Establishing a framework programme on security and safeguarding liberties for the period 2007-2013' (COM(2005) 124 final), Brussels, 6 April 2005.

European Commission, Commission communication, 'Concerning terrorist recruitment: addressing the factors contributing to violent radicalisation' (COM(2005) 313 final), Brussels, 21 September 2005.

European Commission, Commission communication, 'European programme for critical infrastructure protection' (COM(2006) 786 final), Brussels, 12 December 2006.

European Commission, Commission communication, 'European space policy' (COM(2007) 212 final), Brussels, 26 April 2007.

European Commission, Commission communication, 'Public-private dialogue in security research and innovation' (COM(2007) 511 final), Brussels, 11 September 2007.

European Commission, Commission communication, 'A strategy for a stronger and more competitive European defence industry' (COM(2007) 764 final), Brussels, 5 December 2007.

European Commission, Commission communication, 'The raw materials initiative — meeting our critical needs for growth and jobs in Europe' (COM(2008) 699 final), Brussels, 4 November 2008.

European Commission, Commission communication, 'Strengthening chemical, biological, radiological and nuclear security in the European Union — an EU CBRN action plan' (COM(2009) 273 final), Brussels, 24 June 2009.

European Commission, Commission communication, 'Towards the integration of maritime surveillance' (COM(2009) 538 final), Brussels, 15 October 2009.

European Commission, Commission communication, 'A European security research and innovation agenda — Commission's initial position on ESRI's key findings and recommendations' (COM(2009) 691 final), Brussels, 21 December 2009.

European Commission, Commission communication, 'The EU internal security strategy in action: five steps towards a more secure Europe' (COM(2010) 673 final), Brussels, 22 November 2010.

European Commission, Commission communication, 'Tackling the challenges in commodity markets and on raw materials' (COM(2011) 25 final), Brussels, 2 February 2011.

European Commission, Commission communication, 'Roadmap to a resource efficient Europe' (COM(2011) 571 final), Brussels, 20 September 2011.

European Commission, Commission communication, 'Innovation for a sustainable future — the eco-innovation action plan (Eco-AP)' (COM(2011) 899 final), Brussels, 15 December 2011.

European Commission, Commission communication, 'Towards a more competitive and efficient defence sector' (COM(2013) 542 final), Brussels, 24 July 2013.

European Commission, Commission communication, 'Preventing radicalisation to terrorism and violent extremism: strengthening the EU's response' (COM(2013) 941 final), Brussels, 15 January 2014.

European Commission, Commission communication, 'For a European industrial renaissance' (COM(2014) 14 final), Brussels, 22 January 2014.

European Commission, Commission communication, 'New EU approach to the detection and mitigation of CBRN-E risks' (COM(2014) 247 final), Brussels, 5 May 2014.

European Commission, Commission communication, 'Review of the list of critical raw materials for the EU and the implementation of the raw materials initiative' (COM(2014) 297 final), Brussels, 26 May 2014.

European Commission, Commission communication, 'European energy security strategy' (COM(2014) 330 final), Brussels, 28 May 2014.

European Commission, Commission communication, 'A framework strategy for a resilient energy union with a forward-looking climate change policy' (COM(2015) 80 final), Brussels, 25 February 2015.

European Commission, Commission communication, 'The European agenda on security' (COM(2015) 185 final), Strasbourg, 28 April 2015.

European Commission, Commission communication, 'A European agenda on migration' (COM(2015) 240 final), Brussels, 13 May 2015.

European Commission, Commission communication, 'Closing the loop — an EU action plan for the circular economy' (COM(2015) 614 final), Brussels, 2 December 2015.

European Commission, Commission communication, 'Action plan for strengthening the fight against terrorist financing' (COM(2016) 50 final), Strasbourg, 2 February 2016.

European Commission, Commission communication, 'Proposal for a regulation establishing an entry/exit system (EES) to register entry and exit data and refusal of entry data of third country nationals crossing the external borders of the Member States of the European Union and determining the conditions for access to the EES for law enforcement purposes and amending Regulation (EC) No 767/2008 and Regulation (EU) No 1077/2011' (COM(2016) 194 final), Brussels, 6 April 2016.

European Commission, Commission communication, 'Proposal for a regulation amending Regulation (EU) 2016/399 as regards the use of the Entry/Exit System' (COM(2016) 196 final), Brussels, 6 April 2016.

European Commission, Commission communication, 'Supporting the prevention of radicalisation leading to violent extremism' (COM(2016) 379 final), Brussels, 14 June 2016.

European Commission, Commission communication, 'Strengthening Europe's cyber resilience system and fostering a competitive and innovative cybersecurity industry' (COM(2016) 410 final), Brussels, 5 July 2016.

European Commission, Commission communication, 'Space strategy for Europe' (COM(2016) 705 final), Brussels, 26 October 2016.

European Commission, Commission communication, 'Proposal for a Regulation establishing a European Travel Information and Authorisation System (ETIAS) and amending Regulations (EU) No 515/2014, (EU) 2016/399, (EU) 2016/794 and (EU)2016/1624' (COM(2016) 731 final), Brussels, 16 November 2016.

European Commission, Commission communication, 'European defence action plan' (COM(2016) 950 final), Brussels, 30 November 2016.

European Commission, Commission communication, 'Proposal for a Regulation of the European Parliament and of the Council on the establishment, operation and use of the Schengen Information System (SIS) in the field of border checks, amending Regulation (EU) No 515/2014 and repealing Regulation (EC) No 1987/2006' (COM(2016) 882 final), Brussels, 21 December 2016.

European Commission, Commission communication, 'Launching the European Defence Fund' (COM(2017) 295 final), Brussels, 7 June 2017.

European Commission, Commission communication, 'Ninth progress report towards an effective and genuine security union' (COM(2017) 407 final), Brussels, 26 July 2017.

European Commission, Commission communication, 'Tenth progress report towards an effective and genuine security union' (COM(2017) 466 final), Brussels, 7 September 2017.

European Commission, Commission communication, 'Investing in a smart, innovative and sustainable industry: a renewed EU industrial policy strategy' (COM(2017) 479 final), Brussels, 13 September 2017.

European Commission, Commission communication, '2017 list of critical raw materials for the EU' (COM(2017) 490 final), Brussels, 13 September 2017.

European Commission, Commission communication, 'Making the most of NIS — towards the effective implementation of Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union' (COM(2017) 476 final/2), Brussels, 4 October 2017.

European Commission, Commission communication, 'Eleventh progress report towards an effective and genuine security union' (COM(2017) 608 final), Brussels, 18 October 2017.

European Commission, Commission communication, 'Action plan to enhance preparedness against chemical, biological, radiological and nuclear security risks' (COM(2017) 610 final), Brussels, 18 October 2017.

European Commission, Commission communication, 'Action plan to support the protection of public spaces' (COM(2017) 612 final), Brussels, 18 October 2017.

European Commission, Commission communication, 'Thirteenth progress report towards an effective and genuine security union' (COM(2018) 46 final), Brussels, 24 January 2018.

European Commission, Commission communication, 'A modern budget for a union that protects, empowers and defends: The multiannual financial framework for 2021-2027' (COM(2018) 321 final), Brussels, 2 May 2018.

European Commission, Commission communication, 'Proposal for a Regulation on the European Border and Coast Guard and repealing Council Joint Action No 98/700/JHA, Regulation (EU) No 1052/2013 of the European Parliament and of the Council and Regulation (EU) No 2016/1624 of the European Parliament and of the Council' (COM(2018) 631 final), Brussels, 12 September 2018.

European Commission, Commission communication, 'Eighteenth progress report towards an effective and genuine security union' (COM(2019) 145 final), Brussels, 23 March 2019.

Commission Decision of 22 April 2005 establishing the European Security Research Advisory Board (2005/516/EC), OJ L 191, 22.7.2005, p. 70-72.

Commission Decision of 27 August 2007 implementing Decision No 574/2007/EC of the European Parliament and of the Council as regards the adoption of strategic guidelines for 2007 to 2013 (2007/599/EC), OJ L 233, 5.9.2007, p. 3-6.

European Commission, Commission decision on the financing of the preparatory action on defence research and the use of unit costs for the year 2017 (C(2017) 2262 final), Brussels, 11 April 2017.

European Commission, Commission decision setting-up the high-level commission expert group on radicalisation (C(2017) 5149 final), Brussels, 27 July 2017.

European Commission, Commission decision on the adoption of the work programme for 2018 and on the financing of the preparatory action on defence research, and authorising the use of unit costs under the preparatory action (C(2018) 1383 final), Brussels, 9 March 2018.

European Commission, Commission decision on the financing of the preparatory action on defence research and the adoption of the work programme for 2019 (C(2019) 1873 final), Brussels, 19 March 2019.

European Commission, draft regulation laying down rules and procedures for the operation of unmanned aircraft, Brussels.

European Commission, Commission recommendation on coordinated response to large scale cybersecurity incidents and crises (C(2017) 6100 final), Brussels, 13 September 2017.

European Commission, Commission recommendation on cybersecurity in the energy sector (C(2019) 2400 final), Brussels, 3 April 2019.

European Commission, 'Green Paper on a European programme for critical infrastructure protection' COM(2005) 576 final, Brussels, 17 November 2005.

European Commission, 'Proposal for a Council Decision on a Critical Infrastructure Warning Information Network (CIWIN)' (COM(2008) 676 final), Brussels, 27 October 2008.

European Commission, 'Proposal for a Regulation of the European Parliament and the Council on risk-preparedness in the electricity sector and repealing Directive 2005/89/EC' (COM(2016) 862 final), Brussels, 30 November 2016

European Commission, 'Proposal for a Regulation establishing the European Defence Industrial Development Programme aiming at supporting the competitiveness and innovative capacity of the EU defence industry' (COM(2017) 294 final), Brussels, 7 June 2017.

European Commission, 'Proposal for a Regulation of the European Parliament and of the Council of the European Union on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification ("Cybersecurity Act")' (COM(2017) 477 final/2), Brussels, 4 October 2017.

European Commission, 'Proposal for a Regulation establishing the space programme of the Union and the European Union Agency for the Space Programme and repealing Regulations (EU) No 912/2010, (EU) No 1285/2013, (EU) No 377/2014 and Decision 541/2014/EU' (COM(2018) 447 final), Brussels, 6 June 2018.

European Commission, 'Proposal for a Regulation of the European Parliament and of the Council establishing Horizon Europe — the Framework Programme for Research and Innovation, laying down its rules for participation and dissemination' (COM(2018) 435 final), Brussels, 7 June 2018.

European Commission, 'Proposal for a Regulation of the European Parliament and of the Council of the European Union establishing the European Defence Fund' (COM(2018) 476 final), Brussels, 13 June 2018.

European Commission, 'Proposal for a Regulation of the European Parliament and of the Council of the European Union establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres' (COM(2018) 630 final), Brussels, 12 September 2018.

European Commission, 'Reflection paper on the future of European defence' (COM(2017) 315 final), Brussels, 7 June 2017.

European Commission, Commission report, *Evaluations of the Competitiveness and Innovation Framework Programme* (COM(2013) 2 final), Brussels, 15 January 2013.

European Commission, Commission report, *Implementation of the Raw Materials Initiative* (COM(2013) 442 final), Brussels, 24 June 2013.

European Commission, Commission report, *A New Deal for European Defence* (COM(2014) 387 final), Brussels, 24 June 2014.

European Commission, Commission report, Ex-post evaluation report for the period 2007-2013 of actions financed by the 'Prevention and fight against crime' programme (ISEC) and the 'Prevention, preparedness and consequence management of terrorism and other security related risks' programme (CIPS) (COM(2018) 455 final), Brussels, 12 June 2018.

European Commission, Commission staff working document, 'Health security in the European Union and internationally' (SEC(2009) 1622 final), Brussels, 23 November 2009.

European Commission, Commission staff working document, 'Review of the European programme for critical infrastructure protection (EPCIP)' (SWD(2012) 190 final), Brussels, 22 June 2012.

European Commission, Commission staff working document, 'A new approach to the European programme for critical infrastructure protection: making European critical infrastructures more secure' (SWD(2013) 318 final), Brussels, 28 August 2013.

European Commission, Commission staff working document, 'Comprehensive assessment of EU security policy' (SWD(2017) 278 final), Brussels, 26 July 2017.

European Commission, Commission staff working document, 'Ex-post evaluation of the "Prevention, Preparedness and Consequence Management of Terrorism and other Security related risks" 2007-2013 Programme (CIPS)' (SWD(2018) 331 final), accompanying Commission report COM(2018) 455 final, Brussels, 12 June 2018.

European Commission, 'White Paper: space — a new European frontier for an expanding Union: an action plan for implementing the European space policy' (COM(2003) 673 final), Brussels, 11 November 2003.

European Commission and High Representative of the Union for Foreign Affairs and Security Policy

European Commission and High Representative of the Union for Foreign Affairs and Security Policy, joint communication, 'Cybersecurity strategy of the European Union: an open, safe and secure cyberspace' (JOIN(2013) 1 final), Brussels, 7 February 2013.

European Commission and High Representative of the Union for Foreign Affairs and Security Policy, joint communication, 'Joint framework on countering hybrid threats: a European Union response' (JOIN(2016) 18 final), Brussels, 6 April 2016.

European Commission and High Representative of the Union for Foreign Affairs and Security Policy, joint staff working document, 'EU operational protocol for countering hybrid threats: "EU Playbook"' (SWD(2016) 227 final), Brussels, 5 July 2016.

European Commission and High Representative of the Union for Foreign Affairs and Security Policy, joint report, *The implementation of the joint framework on countering hybrid threats — A European Union response* (JOIN(2017) 30 final), Brussels, 19 July 2017.

European Commission and High Representative of the Union for Foreign Affairs and Security Policy, joint communication, 'Resilience, deterrence and defence: building strong cybersecurity for the EU' (JOIN(2017) 450 final), Brussels, 13 September 2017.

European Commission and High Representative of the Union for Foreign Affairs and Security Policy, joint report, *The implementation of the joint framework on countering hybrid threats from July 2017 to June 2018* (JOIN(2018) 14 final), Brussels, 13 June 2018.

European Parliament

European Parliament Resolution 2008/2030(INI) on space and security, Strasbourg, 10 July 2008.

European Parliament Resolution 2013/2105(INI) on the implementation of the common security and defence policy (based on the annual report from the Council to the European Parliament on the common foreign and security policy), Strasbourg, 21 November 2013.

European Parliament Resolution 2015/2276(INI) on space capabilities for European security and defence, Strasbourg, 8 June 2016.

European Parliament and Council of the European Union

Decision No 1639/2006/EC of the European Parliament and of the Council of 24 October 2006 establishing a competitiveness and innovation framework programme (2007 to 2013), OJ L 310, 9.11.2006, p. 15-40.

Decision No 1982/2006/EC of the European Parliament and of the Council of 18 December 2006 concerning the seventh framework programme of the European Community for research, technological development and demonstration activities (2007-2013), Brussels, OJ L 412, 30.12.2006, p. 1-43.

Decision No 574/2007/EC of the European Parliament and of the Council of 23 May 2007 establishing the External Borders Fund for the period 2007 to 2013 as part of the general programme 'Solidarity and management of migration flows', OJ L 144, 6.6.2007, p. 22-44.

Decision No 1082/2013/EU of the European Parliament and of the Council of 22 October 2013 on serious cross-border threats to health and repealing Decision No 2119/98/EC, OJ L 293, 5.11.2013, p. 1-15.

Decision No 1313/2013/EU of the European Parliament and of the Council of 17 December 2013 on a Union civil protection mechanism, Brussels, OJ L 347, 20.12.2013, p. 924-947.

Decision No 541/2014/EU of the European Parliament and of the Council of 16 April 2014 establishing a framework for space surveillance and tracking support, OJ L 158, 27.5.2014, p. 227-234.

Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing, OJ L 309, 25.11.2005, p. 15-36.

Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC, OJ L 141, 5.6.2015, p. 73-117.

Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC, OJ L 337, 23.12.2015, p. 35-127.

Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, OJ L 119, 4.5.2016, p. 132-149.

Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, OJ L 194, 19.7.2016, p. 1-30.

Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU, OJ L 156, 19.6.2018, p. 43-74.

Regulation (EC) No 2320/2002 of the European Parliament and of the Council of 16 December 2002 establishing common rules in the field of civil aviation security, OJ L 355, 30.12.2002, p. 1-21.

Regulation (EC) No 1889/2005 of the European Parliament and of the Council of 26 October 2005 on controls of cash entering or leaving the Community, OJ L 309, 25.11.2005, p. 9-12.

Regulation (EC) No 1781/2006 of the European Parliament and of the Council of 15 November 2006 on information on the payer accompanying transfers of funds, OJ L 345, 8.12.2006, p. 1-9.

Regulation (EC) No 300/2008 of the European Parliament and of the Council of 11 March 2008 on common rules in the field of civil aviation security and repealing Regulation (EC) No 2320/2002, OJ L 97, 9.4.2008, p. 72-84.

Regulation (EU) No 912/2010 of the European Parliament and of the Council of 22 September 2010 setting up the European GNSS Agency, repealing Council Regulation (EC) No 1321/2004 on the establishment of structures for the management of the European satellite radio navigation programmes and amending Regulation (EC) No 683/2008, OJ L 276, 20.10.2010, p. 11-21.

Regulation (EU) No 98/2013 of the European Parliament and of the Council of 15 January 2013 on the marketing and use of explosives precursors, OJ L 39, 9.2.2013, p. 1-11.

Regulation (EU) No 1052/2013 of the European Parliament and of the Council of 22 October 2013 establishing the European Border Surveillance System (Eurosur), OJ L 295, 6.11.2013, p. 11-26.

Regulation (EU) No 1287/2013 of the European Parliament and of the Council of 11 December 2013 establishing a programme for the competitiveness of enterprises and small and medium-sized enterprises (COSME) (2014-2020) and repealing Decision No 1639/2006/EC, OJ L 347, 20.12.2013, p. 33-49.

Regulation (EU) No 1291/2013 of the European Parliament and of the Council of 11 December 2013 establishing Horizon 2020 — the Framework Programme for Research and Innovation (2014-2020) and repealing Decision No 1982/2006/EC, Strasbourg, OJ L 347, 20.12.2013, p. 104-173.

Regulation (EU) No 1381/2013 of the European Parliament and of the Council of 17 December 2013 establishing a Rights, Equality and Citizenship Programme for the period 2014 to 2020, OJ L 354, 28.12.2013, p. 62-72.

Regulation (EU) No 1382/2013 of the European Parliament and of the Council of 17 December 2013 establishing a Justice Programme for the period 2014 to 2020, Brussels, OJ L 354, 28.12.2013, p. 73-83.

Regulation (EU) No 377/2014 of the European Parliament and of the Council of 3 April 2014 establishing the Copernicus Programme and repealing Regulation (EU) No 911/2010, OJ L 122, 24.4.2014, p. 44-66.

Regulation (EU) No 513/2014 of the European Parliament and of the Council of 16 April 2014 establishing, as part of the Internal Security Fund, the instrument for financial support for police cooperation, preventing and

combating crime, and crisis management and repealing Council Decision 2007/125/JHA, OJ L 150, 20.5.2014, p. 93-111.

Regulation (EU) No 515/2014 of the European Parliament and of the Council of 16 April 2014 establishing, as part of the Internal Security Fund, the instrument for financial support for external borders and visa and repealing Decision No 574/2007/EC, OJ L 150, 20.5.2014, p. 143-167.

Regulation (EU) No 516/2014 of the European Parliament and of the Council of 16 April 2014 establishing the Asylum, Migration and Integration Fund, amending Council Decision 2008/381/EC and repealing Decisions No 573/2007/EC and No 575/2007/EC of the European Parliament and of the Council and Council Decision 2007/435/EC, OJ L 150, 20.5.2014, p. 168-194.

Regulation (EU) 2016/399 of the European Parliament and of the Council of 9 March 2016 on a Union Code on the rules governing the movement of persons across borders (Schengen Borders Code), OJ L 77, 23.3.2016, p. 1-52.

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 4.5.2016, p. 1-88.

Regulation (EU) 2017/1938 of the European Parliament and of the Council of 25 October 2017 concerning measures to safeguard the security of gas supply and repealing Regulation (EU) No 994/2010, OJ L 280, 28.10.2017, p. 1-56.

European Parliament, European Council and Council of the European Union

European Parliament, European Council and Council, joint communication, 'Increasing resilience and bolstering capabilities to address hybrid threats' (JOIN(2018) 16 final), Brussels, 13 June 2018.

Abbreviations

ACER	Agency for the Cooperation of Energy Regulators
AI	artificial intelligence
Airpol	EU Airport Police Network
AMIF	Asylum, Migration and Integration Fund
BTWC	Biological and Toxin Weapons Convention
CapTech	capability technology group
CBRN	chemical, biological, radiological, nuclear
CBRN-E	chemical, biological, radiological, nuclear and high-yield explosive
CERT-EU	Computer Emergency Response Team of the European Union
CFSP	common foreign and security policy
CIP	competitiveness and innovation framework programme
CIPRNet	Critical Infrastructure Preparedness and Resilience Research Network
CIPS	the prevention, preparedness and consequence management of terrorism and other security-related risks programme
CISE	Common Information Sharing Environment
CIWIN	Critical Infrastructure Warning Information Network
CoE	centre(s) of excellence
Connect	Directorate-General for Communications Networks, Content and Technology
Cordis	Community Research and Development Information Service
COSME	programme for the competitiveness of enterprises and SMEs
CSDP	Common Security and Defence Policy
CSIRT	Computer Security Incident Response Team
DG	Directorate-General
EASO	European Asylum Support Office
EBF	External Borders Fund
EBSA	European Biosafety Association
EC3	European Cybercrime Centre
ECHO	Directorate-General for European Civil Protection and Humanitarian Aid Operations
ECI	European critical infrastructure(s)
ECTC	European Counter Terrorism Centre
EDA	European Defence Agency
EDF	European Defence Fund
EDIDP	European Defence Industrial Development Programme
EDPS	European Data Protection Supervisor
EEAS	European External Action Service
EEODN	European Explosive Ordnance Disposal Network
EGNOS	European Geostationary Navigation Overlay Service
EIP	European innovation partnership

EIT	European Institute of Innovation and Technology
EMSA	European Maritime Safety Agency
ENISA	European Union Agency for Cybersecurity
Enlets	European Network of Law Enforcement Technology Services
EPCIP	European programme for critical infrastructure protection
Erncip	European Reference Network for Critical Infrastructure Protection
ESA	European Space Agency
ESDP	European security and defence policy
ESRAB	European Security Research Advisory Board
ESRIA	European security research and innovation agenda
ESRIF	European Security Research and Innovation Forum
ESRP	European security research programme
ETIAS	European Travel Information and Authorisation System
ETSI	European Telecommunications Standards Institute
EU	European Union
EU IRU	European Union Internet Referral Unit
EUISS	European Union Institute for Security Studies
eu-LISA	European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice
EUMETSAT	European Organisation for the Exploitation of Meteorological Satellites
EUMSS	European Union maritime security strategy
Eurodac	European Asylum Dactyloscopy Database
Europol	European Union Agency for Law Enforcement Cooperation
Eurosur	European Border Surveillance System
FATF	Financial Action Task Force
FP7	Seventh framework programme for research and technological development
Frontex	European Border and Coast Guard Agency
GHSA	Global Health Security Agenda
GNSS	global navigation satellite system(s)
GPS	Global Positioning System
GSA	European Global Navigation Satellite Systems Agency
H2020	Horizon 2020
HR/VP	High Representative of the Union for Foreign Affairs and Security Policy and Vice-President of the Commission
IAEA	International Atomic Energy Agency
IcSP	Instrument contributing to Stability and Peace
ICT	information and communication technology
IFBA	International Federation of Biosafety Associations
IMF	International Monetary Fund
Interpol	International Criminal Police Organisation

IoT	internet of things
ISEC	prevention of and fight against crime programme
ISF	Internal Security Fund
ISIL	Islamic State in Iraq and the Levant
ISIS	Islamic State in Iraq and Syria
ITU	United Nations International Telecommunication Union
JITs	Joint Investigation Teams
JRC	Joint Research Centre
KET	key enabling technology
MFF	multiannual financial framework
MO	modus operandi
MSB	money service business
NATO	North Atlantic Treaty Organization
NCCF	Natural Capital Financing Facility
NEO	near-Earth objects
NGO	non-governmental organisation
NIS	network and information security
OECD	Organisation for Economic Co-operation and Development
OIE	World Organisation for Animal Health
OSCE	Organization for Security and Co-operation in Europe
PADR	preparatory action on defence research
PASR	preparatory action on security research
PCEI	protection of critical energy infrastructures
PESCO	permanent structured cooperation
PF4EE	Private Finance for Energy Efficiency
PNR	passenger name record(s)
PNT	positioning, navigation and timing
R & D	research and development
R & T	research and technological development
Railpol	European Network of Railway Police Forces
SatCen	European Union Satellite Centre
SIS	Schengen Information System
SMEs	small and medium-sized enterprises
SoC/SiP	system-on-a-chip/system-in-a-package
SSA	space situational awareness
SST	space surveillance and tracking
TFEU	Treaty on the Functioning of the European Union
TFTP	Terrorist Finance Tracking Program
UAV	unmanned aerial vehicle

UN	United Nations
UNDP	United Nations Development Programme
UNODC	United Nations Office on Drugs and Crime
VIS	Visa Information System
WHO	World Health Organization
WMO	World Meteorological Organization
ACER	Agency for the Cooperation of Energy Regulators
AIRPOL	EU Airport Police Network
BTWC	Biological and Toxin Weapons Convention
C2	Command and Control
CBRN-E	Chemical, biological, radiological, nuclear and high-yield explosive
CCDCOE	Cooperative Cyber Defence Centre of Excellence
CEAS	Common European Asylum System
CERT-EU	Computer Emergency Response Team of the European Union
CF SEDSS	Consultation Forum for Sustainable Energy in the Defence and Security Sector
CFSP	Common Foreign and Security Policy
CI	Critical infrastructure
CIPRNet	Critical Infrastructure Preparedness and Resilience Research Network
CIWIN	Critical Infrastructure Warning Information Network
CoR	The European Committee of the Regions
cPPP	Contractual public private partnership
CRM	Critical raw material
CSDP	Common Security and Defence Policy
CWC	Chemical Weapons Convention
DG CNECT	Directorate-General for Communications Networks, Content and Technology
DG DEVCO	Directorate-General for International Cooperation and Development
DG ECHO	Directorate-General for European Civil Protection and Humanitarian Aid Operations
DG ENER	Directorate-General for Energy
DG ENV	Directorate-General for Environment
DG GROW	Directorate-General for Internal Market, Industry, Entrepreneurship and SMEs
DG HOME	Directorate-General for Migration and Home Affairs
DG MARE	Directorate-General for Maritime Affairs and Fisheries
DG MOVE	Directorate-General for Mobility and Transport
DG REGIO	Directorate-General for Regional and Urban Policy
DG RTD	Directorate-General for Research and Innovation
DG SANTE	Directorate-General for Health and Food Safety
DG TRADE	Directorate-General for Trade
EASME	European Agency for Small and Medium-sized Enterprises
EASO	European Asylum Support Office

EBSA	European Biosafety Association
ECDC	European Centre for Disease Prevention and Control
ECI	European Critical Infrastructure
ECTC	European Counter Terrorism Centre
EC3	European Cybercrime Centre
EDA	European Defence Agency
EDAP	European Defence Action Plan
EDIDP	European Defence Industrial Development Programme
EDPS	European Data Protection Supervisor
EDRP	European Defence Research Programme
EEAS	European External Action Service
EFCA	European Fisheries Control Agency
EFSA	European Food Safety Authority
EIP	European Innovation Partnership
EIS	Europol Information System
EISAC	European Infrastructures Simulation & Analysis Centre
EIT	European Institute of Innovation and Technology
EMSA	European Maritime Safety Agency
ENER	European Network of Experts on Radicalisation
ENISA	European Union Agency for Network and Information Security
ENLETS	European Network of Law Enforcement Technology Services
ENSEC CoE	Energy Security Centre of Excellence
EO	Earth Observation
EPE	Europol Platform for Experts
EPCIP	European Programme for Critical Infrastructure Protection
ERDF	European Regional Development Fund
ERECON	European Rare Earth Competency Network
ERNICIP	European Reference Network for Critical Infrastructure Protection
ESDP	European Security and Defence Policy
ESA	European Space Agency
ESS	European Security Strategy
ETIAS	European Travel Information and Authorisation System
ETSI	European Telecommunications Standards Institute
EUGS	EU Global Strategy
EU IRU	European Union Internet Referral Unit
EUISS	European Union Institute for Security Studies
eu-LISA	European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice
EUMSS	European Union Maritime Security Strategy
EURODAC	European Asylum Dactyloscopy Database

EUROPOL	European Police Office
EUROSUR	European Border Surveillance System
EWRS	Early Warning and Response System
FAO	Food and Agriculture Organization of the United Nations
FATF	Financial Action Task Force
FP7	7th Framework Programme for Research and Technological Development
Frontex	European Border and Coast Guard Agency
GDPR	General Data Protection Regulation
GEO	Geostationary orbit
GHSA	Global Health Security Agenda
GHSI	Global Health Security Initiative
GNSS	Global Navigation Satellite System
GOVSATCOM	Governmental Satellite Communications
GPS	Global Positioning System
GSA	European Global Navigation Satellite Systems Agency
HES	Higher or Secondary Education Establishments
HR	High Representative
IAEA	International Atomic Energy Agency
IcSP	Instrument contributing to Stability and Peace
ICTs	Information and communication technologies
IFBA	International Federation of Biosafety Associations
IMF	International Monetary Fund
IMINT	Imagery Intelligence
INSC	Instrument for Nuclear Safety Cooperation
INTCEN	EU Intelligence and Situation Centre
INTERPOL	International Criminal Police Organisation
ISACs	Sectorial Information Sharing and Analysis Centres
ISF	Internal Security Fund
ISIL	Islamic State in Iraq and the Levant
ISIS	Islamic State in Iraq and Syria
ISS	Internal Security Strategy
ITU	United Nation International Telecommunication Union
J-CAT	Cybercrime Action Taskforce
JISD	Joint Intelligence and Security Division of NATO
JITs	Joint Investigation Teams
JRC	Joint Research Centre
KETs	Key Enabling Technologies
MFF	Multiannual financial framework
MS	Member State

NATO	North Atlantic Treaty Organisation
NIS	Network and information security
OECD	Organisation for Economic Co-operation and Development
OIE	Office international des épizooties
OPCW	Organisation for the Prohibition of Chemical Weapons
OSCE	Organisation for Security and Cooperation in Europe
OSP	Operator Security Plan
PADR	Preparatory Action for Defence Research
PCEI	Protection of critical energy infrastructures
PESCO	Permanent Structured Cooperation
PNR	EU Passenger Name Records
PPP	Public private partnership
R&D	Research and development
R&T	Research and technological development
RAILPOL	European Network of Railway Police Forces
RAN	Radicalisation Awareness Network
RPAS	Remotely piloted airborne systems
SatCen	European Union Satellite Centre
SATCOM	Satellite Communications
SG	Secretary-General of the European Commission
SIENA	Secure Information Exchange Network Application
SIS II	Schengen Information System
SoC/SiP	System-on-a-Chip/System-in-Package
SSA	Space Situational Awareness
SWE	Space Weather
TFEU	Treaty on the Functioning of the European Union
TNCEIP	Thematic Network on Critical Energy Infrastructure Protection
UAS	Unmanned aircraft systems
UAV	Unmanned aircraft vehicles
UN	United Nations
UNDP	United Nations Development Programme
UNICRI	United Nations Interregional Crime and Justice Research Institute
UNODC	United Nations Office on Drugs and Crime
VDES	Vessel Data Exchange System
VIS	Visa Information System
VP	Vice-President
WHO	World Health Organisation
WMD	Weapons of mass destruction

Country codes:

AL	Albania	LT	Lithuania
AT	Austria	LU	Luxembourg
AU	Australia	LV	Latvia
BA	Bosnia and Herzegovina	MD	Moldova
BE	Belgium	MK	North Macedonia
BG	Bulgaria	ML	Mali
BR	Brazil	MT	Malta
CH	Switzerland	MY	Malaysia
CN	China	NL	Netherlands
CU	Cuba	NO	Norway
CY	Cyprus	PL	Poland
CZ	Czechia	PT	Portugal
DE	Germany	RO	Romania
DK	Denmark	RS	Serbia
EE	Estonia	RU	Russia
EL	Greece	SE	Sweden
ES	Spain	SG	Singapore
FI	Finland	SI	Slovenia
FR	France	SK	Slovakia
GE	Georgia	TH	Thailand
GI	Gibraltar	TN	Tunisia
HK	Hong Kong	TR	Turkey
HR	Croatia	TW	Taiwan
HU	Hungary	UA	Ukraine
IE	Ireland	UK	United Kingdom
IL	Israel	US	United States
IN	India	VN	Vietnam
IS	Iceland	XK	Kosovo
IT	Italy	YE	Yemen
KR	South Korea	ZA	South Africa

List of figures

Figure 1: Key suppliers of critical raw materials (CRMs) for advanced Lithium-ion batteries, fuel cells, robotics, drones and 3D printing	30
Figure 2: Historical timeline of the EU security strategies	94
Figure 3: Missions and cross-cutting areas of security research under FP7	99
Figure 4: Structure of Horizon 2020	103
Figure 5: Distribution of H2020 budget.....	104
Figure 6: Proposed structure of Horizon Europe	111
Figure 7: Overview of European security research, including advisory bodies.....	113
Figure 8: Differences between R & T and R & D in terms of technology readiness levels (TRLs).....	116
Figure 9: Structure and details of the European Defence Fund	119
Figure 10: Overview of the evolution of European Defence Research under EU funds and associated legislation.....	122
Figure 11: Proportions of projects by building block (%).....	129
Figure 12: Distribution of projects by number of building blocks to which they contribute (%)	129
Figure 13: Breakdown of projects by building block.....	130
Figure 14: Proportions of projects by priority (%).....	130
Figure 15: Distribution of projects by number of priorities to which they contribute (%).....	131
Figure 16: Distribution of projects by priorities and building blocks (%)	131
Figure 17: Numbers of projects by main focus	132
Figure 18: Numbers of projects by priority and main focus.....	133
Figure 19: Numbers of projects funded under Programme 3.7 and under other programmes	135
Figure 20: Numbers of projects by H2020 funding programme.....	136
Figure 21: Distribution of projects by building block and funding programme.....	136
Figure 22: Numbers of projects to which EU Member States contribute.....	137
Figure 23: Numbers of projects to which non-EU countries contribute	138
Figure 24: Numbers of contributing organisations by legal status	138
Figure 25: Numbers of contributions from organisations by legal status	139
Figure 26: Distribution of contributions from organisations by legal status and by building block	140
Figure 27: Distribution of contributions from organisations by legal status and by priority	140
Figure 28: Numbers of projects by building block and dual-use potential	141
Figure 29: Numbers of projects by priority and dual-use potential.....	141
Figure 30: Overview of JRC actions and deliverables in the area of border control, 2018.....	143
Figure 31: Overview of JRC actions and deliverables in the area of critical infrastructure, 2018.....	144
Figure 32: Overview of JRC actions and deliverables in the area of protection of public spaces, 2018-2019	145
Figure 33: Overview of JRC actions and deliverables in the area of critical supplies, 2018-2020	146
Figure 34: Overview of JRC actions and deliverables in the area of cybersecurity, 2018	148

Figure 35: Overview of JRC actions and deliverables in the area of CBRN-E, 2018	150
Figure 36: Overview of JRC actions and deliverables in the area of hybrid threats, 2018.....	151
Figure 37: Overview of JRC actions and deliverables in the area of space, 2018.....	152
Figure 38: Horizon scanning mapping and prioritisation	159

List of tables

Table 1: Non-exhaustive list of assaults against various types of public spaces in Europe in recent years, indicating the modus operandi (MO).....	23
Table 2: Timeline of implementation of the EU cyberdefence policy framework.....	38
Table 3: Distribution of projects, participation and funding in FP7 security research.....	99
Table 4: The ESRIA research content clusters and cluster components.....	100
Table 5: Distribution of budget for Societal challenges under H2020 ⁽³⁶⁾	104
Table 6: Evolution of topics in the Horizon 2020 Secure Societies work programmes (WPs).....	105
Table 7: Defence research projects funded using the EU budget: pilot project and preliminary action (updated in December 2018).....	123
Table 8: Structure of Horizon 2020 funding by programme, including a breakdown of the 'Secure societies' programme (Programme 3.7, in red).....	134
Table 9: Horizon scanning: security issues by main overarching discipline.....	163
Table 10: Horizon scanning: security issues by main topical aspects.....	164
Table 11: Distribution of projects by building block.....	222
Table 12: Distribution of projects by number of building blocks to which they contribute.....	222
Table 13: Number of projects related to different building block.....	223
Table 14: Distribution of projects by priority.....	224
Table 15: Distribution of projects by number of priorities to which they contribute.....	224
Table 16: Distribution of projects by priority and building block.....	224
Table 17: Number of projects by main focus.....	225
Table 18: Number of projects by building block and main focus.....	226
Table 19: Number of projects by priority and main focus.....	230
Table 20: Number of projects funded under Programme 3.7 and under other programmes.....	232
Table 21: Number of projects per H2020 funding programme.....	233
Table 22: Distribution of projects by building block and funding programme.....	234
Table 23: Number of projects to which countries contribute.....	234
Table 24: Number of projects by building block to which countries contribute.....	236
Table 25: Number of contributing organisations by legal status.....	246
Table 26: Number of contributions from organisations by legal status and role.....	246
Table 27: Number of contributions from organisations by building block, legal status and role.....	246
Table 28: Number of contributions from organisations by priority, legal status and role.....	249
Table 29: Number of projects with dual-use potential.....	249
Table 30: Number of projects by priority and dual-use potential.....	250
Table 31: Number of projects by building block and dual-use potential.....	250
Table 32: Entities participating in at least 2 projects related to "Border control".....	251
Table 33: Entities participating in at least 2 projects related to "CBRN-E".....	252
Table 34: Entities participating in at least 2 projects related to "Combating radicalisation".....	252

Table 35: Entities participating in at least 2 projects related to "Critical infrastructures"	252
Table 36: Entities participating in projects related to "Critical supplies"	253
Table 37: Entities participating in at least 4 projects related to "Cybersecurity"	254
Table 38: Entities participating in at least 2 projects related to "Defence"	255
Table 39: Entities participating in projects related to "Hybrid threats"	255
Table 40: Entities participating in at least 2 projects related to "Public spaces"	256
Table 41: Entities participating in projects related to "Space"	257
Table 42: Entities participating in at least 2 projects related to "Terrorism financing"	258

Annexes

Annex 1. List of European critical infrastructure sectors as listed in Directive 2008/114/EC

Sector	Subsector	
I Energy	1. Electricity	Infrastructures and facilities for generation and transmission of electricity in respect of supply electricity
	2. Oil	Oil production, refining, treatment, storage and transmission by pipelines
	3. Gas	Gas production, refining, treatment, storage and transmission by pipelines Liquefied natural gas terminals
II Transport	4. Road transport	
	5. Rail transport	
	6. Air transport	
	7. Inland waterways transport	
	8. Ocean and short-sea shipping and ports	

Annex 2. Examples of critical infrastructure disruptions

Below are given examples of critical infrastructure disruptions due to accidental, natural, or intentional causes. Unless specified, they are taken from Setola et al. (2016)

Year	Critical infrastructure disruptions
2001	On 18 July 2001, train wagons containing chloride acid derailed in a downtown tunnel in Baltimore, the United States. Firefighters, in the absence of information about the presence of chloride acid on the train, decided to let the train burn. Also unknown was that a high-pressure water mains, a set of glass fibres and a power transmission cable were located close to the same tunnel. Because of the fire, the water transport pipeline to downtown burst open. As a result, over 70 million gallons of water flooded downtown streets and houses, the drinking water supply failed and the firefighters lost their water supply. Glass fibres melted and caused a noticeable worldwide slowdown of the internet as well as local and international telephony outages. Over 1 200 buildings lost power.

Year	Critical infrastructure disruptions
2001	<p>The collapse of the World Trade Center owing to the events of 9/11 caused the inoperability of many infrastructures (electricity, water, gas, communication, steam distribution, etc.) in a large area of Manhattan. Moreover, the presence in that area of important telecommunication nodes induced degradation in telecommunication and internet availability outside the United States. This major impact was caused by the co-location of a multitude of vital critical infrastructures inside the World Trade Center. In those buildings were hosted the Port Authority Emergency Management Center, the Office of Emergency Management Operations Center, electrical power substations, steam and gas distribution facilities and metro stations. Moreover, the emergency operations were affected by such extreme co-location. For instance, the Verizon building at 140 West Street, contained 306 000 telephony and over 55 000 data lines from 30 operators and provided services to 34 000 customers in lower Manhattan. A set of these lines was connected to antennae for first responders and mobile telephony on the roofs of the World Trade Centre towers and adjacent buildings. Communication capacity for the first responders was almost immediately lost because of fire and the collapse of the towers. Data and telephony services failed as the Verizon building became damaged by falling debris. Lines were cut and backup power was lost because of the flooding of batteries. Many of the communication backup lines for first responders and agencies involved in disaster management were co-located with the primary circuits and failed. The remaining fixed and wireless communication for emergency response failed, as police did not allow Verizon to refill the fuel tanks for their backup power generators at two other, still operational, communication switch locations. During the recovery phase, police did not allow crews of all co-located operators to enter the closed-off area; only Verizon crews were allowed to work on repairs. By wearing Verizon T-shirts, AT&T repair crews and crews from other telecommunication companies were able to enter the area and perform their work.</p>
2004	<p>During the night of 31 December there was a problem with the air-conditioning system of an important telecommunication node in Rome, Italy. The problem had not been adequately managed, causing an increased degradation up to the complete collapse of the node. The operator had no way of predicting which services would be impacted by the failure. It decided to not provide any warning while trying to solve the problem internally. Unfortunately, it was unable to manage the situation. The direct consequence was the cessation for 6 hours of all wired and mobile telephone communication in a large area of Rome. And, as an indirect consequence, more than 5 000 banks and 3 000 postal offices nationwide were without communications. In addition, 70% of check-in desks at Rome airport were inoperable. Finally, a blackout nearly occurred because the electrical distribution system operators abruptly lost the ability to supervise and manage half of Rome's power grid.</p>
2010	<p>In mid-April 2010, the Eyjafjallajökull volcano in Iceland erupted through a fast-cooling ice cap (a so-called VEI 4 class eruption). As a result, glass particles were blown into the air and transported to Europe in several waves during a month. Depending on the jet stream, some 30 European nations had to close down their airspace, affecting hundred thousands of passengers. Just-in-time transport by plane, for example of repair parts and of medicines and donor organs for transplantation, could not take place. The financial loss for the tourist sector was EUR 1 billion. The air transport industry lost EUR 1.5-2.5 billion. The worldwide impact on gross domestic product was USD 5 billion.</p>
2015 and 2017 (Styczinski et al., 2016)	<p>On 23 December 2015, three Ukrainian electricity distribution companies suffered widespread power outages due to a cyberattack. In the first known cyber-enabled disruption of electricity service, the attacks were executed every 30 minutes and resulted in outages for 225 000 customers for 1-6 hours. An investigation is under way regarding a second attack on Ukraine's power grid that resulted in parts of the capital, Kiev, being without power on 17-18 December 2016. The attackers hijacked distribution-level industrial control systems and issued commands through a human-machine interface that resulted in power outages. Meanwhile, the attackers locked out the grid operators to diminish the operators' ability to override the attack.</p>
2016	<p>On 4 January 2016, a special weather condition caused a layer of 5 cm of black ice in the north of the Netherlands, which impacted various critical infrastructures for several days. High voltage lines develop a 'wing profile', causing dangling of the lines, with power dips as a result. Hospitals regarded the risk of power outages as too high and stopped all non-essential surgeries. Schools were closed. Road and rail transport was generally not possible. Milk collection at farms was halted. Milk products could not be produced and distributed to supermarkets across a large part of the Netherlands. The air force was unable to scramble their F16s.</p>

Annex 3. Permanent structured cooperation projects

This annex lists the 34 approved PESCO projects (see Section 2.11.4), and was taken from <https://pesco.europa.eu/> on 16 April 2019. The projects are ordered under thematic headings.

Training, facilities	— European Union Training Mission Competence Centre (EU TMCC)
	— European Training Certification Centre for European Armies
	— Helicopter Hot and High Training (H3 Training)
	— Joint EU Intelligence School
	— EU Test and Evaluation Centres
Land, formations, systems	— Deployable Military Disaster Relief Capability Package
	— Armoured Infantry Fighting Vehicle / Amphibious Assault Vehicle / Light Armoured
	— Indirect Fire Support Capability (EuroArtillery)
	— EUFOR Crisis Response Operation Core (EUFOR CROC)
	— Integrated Unmanned Ground System (UGS)
	— EU Beyond Line Of Sight (BLOS) Land Battlefield Missile Systems
Maritime	— Maritime (semi) Autonomous Systems for Mine Countermeasures (MAS MCM)
	— Harbour and Maritime Surveillance and Protection (HARMSPRO)
	— Upgrade of Maritime Surveillance
	— Deployable Modular Underwater Intervention Capability Package (Divepack)
Air, systems	— European Medium Altitude Long Endurance Remotely Piloted Aircraft Systems –
	— European Attack Helicopters TIGER Mark III
	— Counter Unmanned Aerial System (C-UAS)
Enabling, joint	— European Medical Command
	— Network of Logistic Hubs in Europe and Support to Operations
	— Military Mobility
	— Energy Operational Function (EOF)
	— Chemical, Biological, Radiological and Nuclear (CBRN) Surveillance as a Service
	— Co-basing
	— Geo-meteorological and Oceanographic (GeoMETOC) Support Coordination
Cyber, C4ISR	— European Secure Software defined Radio (ESSOR)
	— Cyber Threats and Incident Response Information Sharing Platform
	— Cyber Rapid Response Teams and Mutual Assistance in Cyber Security
	— Strategic Command and Control (C2) System for CSDP Missions and Operations
	— European High Atmosphere Airship Platform (EHAAP) – Persistent Intelligence
	— One Deployable Special Operations Forces (SOF) Tactical Command and Control
	— Electronic Warfare Capability and Interoperability Programme for Future Joint
Space	— EU Radio Navigation Solution (EURAS)
	— European Military Space Surveillance Awareness Network (EU-SSA-N)

Annex 4. Horizon 2020 security- and defence-related projects (master table)

Project id	Project acronym	Programme	Project title	Start Date	End Date	Total Cost (€)	EC Max Contribution (€)	Call	Coordinator Country	Participant Countries	Building block(s)	Priority(ies)	Main focus(es)	Dual Use
700829	3D-Forensics/FTI	H2020-EU.3.; H2020-EU.2.	Mobile high-resolution 3D-Scanner and 3D data analysis for forensic evidence fast track to innovation	1/07/2016	31/12/2018	1 582 384	1 219 389	H2020-FTIPilot-2015-1	DE	DE;UK;NL;IT	Other	Organised crime	Law enforcement; Forensics	YES
671562	5G-ENSURE	H2020-EU.2.1.1.3.	5G Enablers for Network and System Security and Resilience	1/11/2015	31/10/2017	7 584 046	7 584 046	H2020-ICT-2014-2	FI	FR;SE;UK;IT;ES;FI	Cybersecurity	Cybercrime	ICT	YES
664354	ADWICE	H2020-EU.4.a.	Advanced Wireless Technologies for Clever Engineering	1/06/2015	31/05/2016	349 687	349 687	H2020-WIDESPREAD-2014-1	CZ	AT	Cybersecurity	Cybercrime		YES
740647	AEGIS	H2020-EU.3.7.6.; H2020-EU.3.7.4.; H2020-EU.3.7.8.	Accelerating EU-US Dialogue for Research and Innovation in CyberSecurity and Privacy	1/05/2017	30/04/2019	744 263	500 000	H2020-DS-SC7-2016	ES	US;IE;IT	Cybersecurity	Cybercrime	Privacy	NO
673751	AIRIMGO	H2020-EU.3.7.; H2020-EU.2.3.1.	ADVANCE IRIS RECOGNITION IN MOVE	1/07/2015	31/12/2015	71 429	50 000	H2020-SMEINST-1-2014	ES		Public spaces; Critical infrastructures	Terrorism & radicalisation	Privacy	YES
740859	ALADDIN	H2020-EU.3.7.6.; H2020-EU.3.7.1.	Advanced holistic Adverse Drone Detection, Identification Neutralization	1/09/2017	31/08/2020	4 998 240	4 998 240	H2020-SEC-2016-2017-1	FR	PL;ES;EL;IT;DE; BE;PT; FR;UK	Critical infrastructures	Terrorism & radicalisation; Organised crime	Law enforcement; UAV	YES
700002	ALFA	H2020-EU.3.7.	Advanced Low Flying Aircrafts Detection and Tracking	1/01/2017	31/12/2019	4 613 831	4 613 831	H2020-BES-2015	AT	NL;DE;ES; PT;IT	Border control; Public spaces; Critical infrastructures	Organised crime; Terrorism & radicalisation	UAV	YES
740972	ALGSTRONGCRYPTO	H2020-EU.1.1.	Algebraic Methods for Stronger Crypto	1/10/2017	30/09/2022	2 447 439	2 447 439	ERC-2016-ADG	NL		Cybersecurity	Cybercrime	Cryptography	YES
669891	AlmaCrypt	H2020-EU.1.1.	Algorithmic and Mathematical Cryptology	1/01/2016	31/12/2020	2 403 125	2 403 125	ERC-2014-ADG	FR	FR	Cybersecurity	Cybercrime	Cryptography	YES
731558	ANASTACIA	H2020-EU.3.7.; H2020-EU.2.1.1.	Advanced Networked Agents for Security and Trust Assessment in CPS/IOT Architectures	1/01/2017	31/12/2019	5 420 209	3 999 209	H2020-DS-LEIT-2016	IT	CH;ES;FR; EL;FI;IT;IE	Cybersecurity	Cybercrime	CPS; IoT	YES
672109	Andrupos	H2020-EU.3.7.; H2020-EU.2.3.1.	Automatic non-destructive recognition of used printing techniques on substrates	1/04/2015	30/09/2015	71 429	50 000	H2020-SMEINST-1-2014	DE	DE;NL	Terrorism financing	Organised crime; Terrorism & radicalisation	Law enforcement; Forensics	YES
700085	ARIES	H2020-EU.3.7.	reliable euRopean Identity EcoSystem	1/09/2016	28/02/2019	2 247 003	2 247 003	H2020-FCT-2015	ES	FR;BE;UK; ES;PT;CZ	Border control; Cybersecurity	Cybercrime; Organised crime	Biometrics; Law enforcement	YES
688237	ARMOUR	H2020-EU.2.1.1.	Large-Scale Experiments of IoT Security Trust	1/02/2016	31/01/2018	1 999 559	1 999 559	H2020-ICT-2015	FR	FR;ES;PT;EL;BE	Cybersecurity	Cybercrime	IoT; ICT	YES
700381	ASGARD	H2020-EU.3.7.	Analysis System for Gathered Raw Data	1/09/2016	29/02/2020	11 992 556	11 992 553	H2020-FCT-2015	ES	SE;DE;BE; AT;ES;IE;EL;NL; FR;CY;PT;FI;IT;UK	Other	Terrorism & radicalisation; Organised crime	Forensics; Law enforcement	YES

Project id	Project acronym	Programme	Project title	Start Date	End Date	Total Cost (€)	EC Max Contribution (€)	Call	Coordinator Country	Participant Countries	Building block(s)	Priority(ies)	Main focus(es)	Dual Use
677917	ASYFAIR	H2020-EU.1.1.	Fair and Consistent Border Controls? A Critical, Multimethodological and Interdisciplinary Study of Asylum Adjudication in Europe	1/09/2016	31/08/2021	1 252 067	1 252 067	ERC-2015-STG	UK		Border control		Ethical dimension	NO
700581	ATENA	H2020-EU.3.7.	Advanced Tools to assess and mitigate the criticality of ICT components and their dependencies over Critical Infrastructures	1/05/2016	30/04/2019	8 111 938	6 889 925	H2020-DS-2015-1	IT	LU;ES;BE;IT;PT;EE;IL	Critical infrastructures; Cybersecurity	Cybercrime		YES
653590	AUGGMED	H2020-EU.3.7.	Automated Serious Game Scenario Generator for Mixed Reality Training	1/06/2015	31/05/2018	5 535 674	5 535 674	H2020-FCT-2014	UK	UK;ES;IL;DE;EL;BE	Other	Terrorism & radicalisation; Organised crime	Law enforcement; Training	YES
781707	Babbler	H2020-EU.3.7.; H2020-EU.2.3.1.	Babbler feasibility study in adjacent market segments.	8/05/2017	7/10/2017	71 429	50 000	H2020-SMEINST-1-2016-2017	NL		Border control	Organised crime	IoT; Supply chain	YES
640110	BASTION	H2020-EU.1.1.	Leveraging Binary Analysis to Secure the Internet of Things	1/03/2015	29/02/2020	1 472 269	1 472 269	ERC-2014-STG	DE		Cybersecurity	Cybercrime	IoT	YES
774802	BlockchainKYC	H2020-EU.3.7.; H2020-EU.2.3.1.	Blockchain-based, 100% automated KYC (Know Your Customer) service	1/07/2017	30/11/2017	71 429	50 000	H2020-SMEINST-1-2016-2017	IS		Cybersecurity	Cybercrime	Biometrics; Blockchain	YES
653676	BODEGA	H2020-EU.3.7.	BORDERGuard - Proactive Enhancement of Human Performance in Border Control	1/06/2015	30/09/2018	4 999 238	4 999 238	H2020-BES-2014	FI	FI;AT;IT;FR;BE;ES;EL	Border control		Ethical dimension	NO
767454	BOTFIND	H2020-EU.1.1.	BOTFIND: Finding Bots, Detect Harassing Automation, and Restoring Trust in Social Media Civic Engagement	1/08/2017	31/01/2019	149 921	149 921	ERC-2017-PoC	UK		Cybersecurity	Cybercrime	Social media	YES
700380	BROADMAP	H2020-EU.3.7.	Mapping Interoperable EU PPDR Broadband Communication Applications and Technology	1/05/2016	30/04/2017	2 169 138	2 169 138	H2020-DRS-2015	BE	FI;BE;IT;NO;HR;BA;IE;SE;RO;DE;EL;ES;IL;FR;NL	Public spaces		Communication technologies; Emergency	YES
700294	C3ISP	H2020-EU.3.7.	Collaborative and Confidential Information Sharing and Analysis for Cyber Protection	1/10/2016	30/09/2019	5 000 045	4 176 446	H2020-DS-2015-1	IT	UK;FR;DE;IT;PL	Cybersecurity	Cybercrime		YES
740736	CAMELOT	H2020-EU.3.7.3.; H2020-EU.3.7.7.	C2 Advanced Multi-domain Environment and Live Observation Technologies	1/05/2017	30/04/2020	9 942 598	8 020 921	H2020-SEC-2016-2017-1	PT	RO;FR;IE;BG;PL;UK;BE;CH;PT;EL;ES	Border control		Surveillance	YES
700540	CANVAS	H2020-EU.3.7.	Constructing an Alliance for Value-driven Cybersecurity	1/09/2016	31/08/2019	1 569 125	1 000 000	H2020-DS-2015-1	CH	ES;CH;IE;DE;BE;FI;NL	Cybersecurity	Cybercrime	Ethical dimension	YES
653748	CARISMAND	H2020-EU.3.7.	Culture And RISK management in Man-made And Natural Disasters	1/10/2015	30/09/2018	3 788 526	3 788 526	H2020-DRS-2014	NL	IT;RO;PT;NL;ES;UK;FR;BG;MT;RS;DE	Other		Disaster management; Ethical dimension	YES
695305	Cathedral	H2020-EU.1.1.	Post-Snowden Circuits and Design Methods for Security	1/09/2016	31/08/2021	2 369 250	2 369 250	ERC-2015-AdG	BE		Cybersecurity	Cybercrime	Cryptography	YES
653323	C-BORD	H2020-EU.3.7.	Effective Container inspection at BORDER control points	1/06/2015	30/11/2018	11 826 453	11 826 453	H2020-BES-2014	FR	PL;FR;UK;NO;IT;DE;NL;HU;BE	Border control; CBRN-E	Organised crime	Supply chain	YES

Project id	Project acronym	Programme	Project title	Start Date	End Date	Total Cost (€)	EC Max Contribution (€)	Call	Coordinator Country	Participant Countries	Building block(s)	Priority(ies)	Main focus(es)	Dual Use
731456	certMILS	H2020-EU.3.7.; H2020-EU.2.1.1.	Compositional security certification for medium-to high-assurance COTS-based systems in environments with emerging threats	1/01/2017	31/12/2020	5 616 544	3 999 056	H2020-DS-LEIT-2016	AT	CZ;DE;ES;AT	Cybersecurity	Cybercrime	Certification; CPS	YES
780075	CHARIOT	H2020-EU.2.1.1.	Cognitive Heterogeneous Architecture for Industrial IoT	1/01/2018	31/12/2020	4 928 563	4 928 563	H2020-IOT-2017	UK	EL;FR;IT;IE;CY;BE	Cybersecurity	Cybercrime	Blockchain; IoT	YES
674716	ChemSniff	H2020-EU.3.7.; H2020-EU.2.3.1.	Chemical sniffer device for multi-mode analysis of threat compounds	1/09/2015	30/04/2018	2 262 000	1 577 030	H2020-SMEINST-2-2014	NL	UK	CBRN-E; Public spaces	Terrorism & radicalisation		YES
700378	CIPSEC	H2020-EU.3.7.	Enhancing Critical Infrastructure Protection with innovative SECurity framework	1/05/2016	30/04/2019	7 017 235	5 258 316	H2020-DS-2015-1	ES	RO;DE;EL; CH;ES;IL;UK;IT	Critical infrastructures; Cybersecurity	Cybercrime; Terrorism & radicalisation	ICT	YES
700665	CITADEL	H2020-EU.3.7.	Critical Infrastructure Protection using Adaptive MILS	1/06/2016	31/05/2019	6 065 267	4 842 819	H2020-DS-2015-1	UK	DE;UK;SE; AT;IT;FR;CZ;NL; ES	Critical infrastructures; Cybersecurity	Cybercrime; Terrorism & radicalisation	ICT	YES
653811	CITYCoP	H2020-EU.3.7.	Citizen Interaction Technologies Yield Community Policing	1/06/2015	31/05/2018	5 576 716	5 576 716	H2020-FCT-2014	NL	IT;BE;DE; RO;FR;AT; UK;PT;NO; MT;ES;RS;BG	Other		Law enforcement; Social sciences	YES
757279	CIVICS	H2020-EU.1.1.	Criminality, Victimization and Social Interactions	1/03/2018	28/02/2023	1 187 046	1 187 046	ERC-2017-STG	NO	NO	Other	Organised crime	Social sciences	NO
700197	CIVILEX	H2020-EU.3.7.	Supporting European Civilian External Actions	1/05/2016	30/04/2017	1 100 351	1 100 351	H2020-BE5-2015	ES	NL;IT;DE;ES	Defence		External security; Information exchange	YES
644024	CLARUS	H2020-EU.2.1.1.3.	A FRAMEWORK FOR USER CENTRED PRIVACY AND SECURITY IN THE CLOUD	1/01/2015	31/12/2017	4 193 548	4 193 548	H2020-ICT-2014-1	ES	FR;DE;ES;UK;BE	Cybersecurity	Cybercrime	Privacy; Cloud; ICT	YES
781400	CLTre	H2020-EU.2.1.1.; H2020-EU.2.3.1.	The Cybersecurity Behavioural Toolkit	1/06/2017	30/11/2017	71 429	50 000	H2020-SMEINST-1-2016-2017	NO		Cybersecurity	Cybercrime	Social sciences	YES
740712	COMPACT	H2020-EU.3.7.4.	COmpetitive Methods to protect local Public Administration from Cyber security Threats	1/05/2017	31/10/2019	4 283 480	3 648 793	H2020-DS-SC7-2016	IT	IT;DE;ES;AT;UK; PT;BE	Cybersecurity	Cybercrime		NO
653454	CREDENTIAL	H2020-EU.3.7.	Secure Cloud Identity Wallet	1/10/2015	30/09/2018	6 686 660	5 978 083	H2020-DS-2014-1	AT	AT;IT;DE;ES;LU; EL;SE	Cybersecurity	Cybercrime	Privacy; Cloud	YES
740723	CS-AWARE	H2020-EU.3.7.4.	A cybersecurity situational awareness and information sharing solution for local public administrations based on advanced big data analysis	1/09/2017	31/08/2020	4 648 363	3 728 604	H2020-DS-SC7-2016	FI	IT;UK;AT;EL;IE; DK;DE;NL	Cybersecurity	Cybercrime		YES
740920	CYBECO	H2020-EU.3.7.4.	Supporting Cyberinsurance from a Behavioural Choice Perspective	1/05/2017	30/04/2019	1 983 510	1 983 510	H2020-DS-SC7-2016	EL	ES;UK;FR;LU;NL	Cybersecurity	Cybercrime	Social sciences	NO
740129	cyberwatchin g.eu	H2020-EU.3.7.6; H2020-EU.3.7.4; H2020-EU.3.7.8.	The European watch on cybersecurity privacy	1/05/2017	30/04/2021	1 999 896	1 999 896	H2020-DS-SC7-2016	UK	IT;BE;ES;CH;UK	Cybersecurity	Cybercrime	Privacy	YES

Project id	Project acronym	Programme	Project title	Start Date	End Date	Total Cost (€)	EC Max Contribution (€)	Call	Coordinator Country	Participant Countries	Building block(s)	Priority(ies)	Main focus(es)	Dual Use
684723	CYPRES	H2020-EU.3.7.; H2020-EU.2.3.1.	CYPRES the ICS and SCADA security companion	1/09/2015	28/02/2018	2 428 706	1 700 094	H2020-SMEINST-2-2015	FR	FR	Critical infrastructures; Public spaces; Cybersecurity	Cybercrime		YES
730843	CYRail	H2020-EU.3.4.8.2.	Cybersecurity in the RAILway sector	1/10/2016	30/09/2018	1 498 150	1 498 150	H2020-S2RJU-OC-2015-01-2	PT	FR;ES;SE;DE	Cybersecurity; Hybrid threats	Terrorism & radicalisation; Cybercrime	Transport	YES
700367	DANTE	H2020-EU.3.7.	Detecting and Analysing TErrorist-related online contents and financing activities	1/09/2016	28/02/2019	6 199 229	4 998 528	H2020-FCT-2015	IT	AT;ES;EL; DE;IT;PT;FR;UK; BE;IE	Terrorism financing; Combating radicalisation	Terrorism & radicalisation	Law enforcement; Social media	YES
725349	DARE	H2020-EU.3.6.1.2.	Dialogue About Radicalisation and Equality	1/05/2017	30/04/2021	4 999 054	4 999 054	H2020-SC6-REV-INEQUAL-2016	UK	HR;NL;RU; TR;DE;UK; NO;PL;MT; FR;TN;BE;EL	Combating radicalisation	Terrorism & radicalisation	Violence; Social sciences	YES
653289	DARWIN	H2020-EU.3.7.	Expecting the unexpected and know how to respond	1/06/2015	31/05/2018	4 998 896	4 998 896	H2020-DRS-2014	NO	SE;IE;IT;IL;DE	Critical infrastructures; Cybersecurity	Cybercrime; Terrorism & radicalisation	Disaster management; Resilience	YES
740898	DEFENDER	H2020-EU.3.7.4.; H2020-EU.3.7.2.	Defending the European Energy Infrastructures	1/05/2017	30/04/2020	8 859 938	6 790 838	CIP-2016-2017-1	IT	SI;IT;DE;RO;FR; UK;IL;PT;EL	Critical infrastructures; Cybersecurity	Cybercrime	CPS; Physical threats	YES
700692	DiSIEM	H2020-EU.3.7.	Diversity Enhancements for SIEMs	1/09/2016	31/08/2019	4 020 019	3 445 876	H2020-DS-2015-1	PT	DE;ES;PT;UK	Cybersecurity	Cybercrime	Cloud	YES
731945	DITAS	H2020-EU.2.1.1.	DITAS: Data-intensive applications Improvement by moving daTA and computation in mixed cloud/fog environmentS	1/01/2017	31/12/2019	4 890 066	4 420 188	H2020-ICT-2016-1	ES	CH;DE;ES; IT;EL;IL	Cybersecurity	Cybercrime	Cloud; ICT	YES
653618	DOGANA	H2020-EU.3.7.	aDvanced sOcial enGineering And vulNerability Assesment Framework	1/09/2015	31/08/2018	5 808 217	4 599 806	H2020-DS-2014-1	IT	AT;FR;BE; UK;DK;IT;IL;EL; PT;CH;RO	Cybersecurity	Cybercrime	Social media	NO
666148	DSTB	H2020-EU.2.1.1.; H2020-EU.2.3.1.	Dyadic Secures The Breach	1/04/2015	31/03/2017	2 882 500	2 017 750	H2020-SMEINST-2-2014	IL		Cybersecurity	Cybercrime	ICT	YES
645421	ECRYPT-CSA	H2020-EU.2.1.1.	European Coordination and Support Action in Cryptology	1/03/2015	28/02/2018	1 000 000	1 000 000	H2020-ICT-2014-1	BE	FR;DE;UK;NL	Cybersecurity; Critical infrastructures	Cybercrime	Cryptography; ICT	YES
643161	ECRYPT-NET	H2020-EU.1.3.1.	European Integrated Research Training Network on Advanced Cryptographic Technologies for the Internet of Things and the Cloud	1/03/2015	28/02/2019	3 893 200	3 893 200	H2020-MSCA-ITN-2014	BE	FR;BE;DE;UK;NL	Cybersecurity	Cybercrime	Cryptography; IoT; Cloud	YES
691025	ENCASE	H2020-EU.1.3.3.	EnhaNcing seCurity And privacy in the Social wEb: a user centered approach for the protection of minors	1/01/2016	31/12/2019	2 160 000	2 160 000	H2020-MSCA-RISE-2015	CY	UK;EL;IT;ES;CY	Cybersecurity	Cybercrime	Social media	YES
740450	ENCIRCLE	H2020-EU.3.7.1.; H2020-EU.3.7.5.	European Cbrn Innovation for the maRket CLuster	10/03/2017	9/03/2021	1 997 085	1 997 085	H2020-SEC-2016-2017-1	BE	FI;IT;UK;FR;PL; DE	CBRN-E	Terrorism & radicalisation		YES
740521	eNOTICE	H2020-EU.3.7.6.; H2020-EU.3.7.2.; H2020-EU.3.7.3.; H2020-EU.3.7.1.;	European Network Of CBRN Tralning CEnters	1/09/2017	31/08/2022	3 587 423	3 497 735	H2020-SEC-2016-2017-1	BE	IT;PL;FR;BE;SE; DE;UK; CZ;TR	CBRN-E	Terrorism & radicalisation		YES

Project id	Project acronym	Programme	Project title	Start Date	End Date	Total Cost (€)	EC Max Contribution (€)	Call	Coordinator Country	Participant Countries	Building block(s)	Priority(ies)	Main focus(es)	Dual Use
		H2020-EU.3.7.7.; H2020-EU.3.7.8.; H2020-EU.3.7.5.												
695022	EPoCH	H2020-EU.1.1.	Exploring and Preventing Cryptographic Hardware Backdoors: Protecting the Internet of Things against Next-Generation Attacks	1/10/2016	30/09/2021	2 498 286	2 498 286	ERC-2015-AdG	DE		Cybersecurity	Cybercrime	Cryptography; IoT	YES
714048	ERNICIP CBRNE STDS 16	H2020-EU.3.7.	ERNICIP thematic group activities in 2016 supporting development of Mandate 487 for standards in security	1/01/2016	31/12/2016	250 000	250 000	H2020-Adhoc-2014-20	BE		Critical infrastructures; CBRN-E	Terrorism & radicalisation		YES
656971	EU and SSR	H2020-EU.1.3.2.	LOCAL OWNERSHIP IN SECURITY SECTOR REFORM ACTIVITIES WITHIN CSDP OPERATIONS OF THE EU	7/10/2015	6/10/2017	183 455	183 455	H2020-MSCA-IF-2014	UK		Defence		External security; Peace keeping; Social sciences	YES
653227	EU-CIVCAP	H2020-EU.3.7.	Preventing and responding to conflict: developing EU CIVilian CAPabilities for a sustainable peace	1/12/2015	30/11/2018	1 714 975	1 714 975	H2020-BES-2014	UK	UK;BE;DK; IT;NL;ES;RS	Defence		External security; Peace keeping	YES
747947	EU-Drones	H2020-EU.1.3.2.	The European Commission in Drone Community: a New Cooperation Area in the Making	1/04/2017	31/03/2019	160 800	160 800	H2020-MSCA-IF-2016	BE		Other		UAV	YES
740507	EUNITY	H2020-EU.3.7.6.; H2020-EU.3.7.4.; H2020-EU.3.7.8.	Cybersecurity and privacy dialogue between Europe and Japan	1/06/2017	31/05/2019	499 813	499 813	H2020-DS-SC7-2016	FR	PL;EL;ES;BE	Cybersecurity	Cybercrime	Privacy	NO
748647	EVACUATION	H2020-EU.1.3.2.	Testing communication strategies to save lives in emergency evacuation	1/03/2018	29/02/2020	195 455	195 455	H2020-MSCA-IF-2016	UK		Public spaces	Terrorism & radicalisation	Emergency	YES
717915	EXTREMDRON	H2020-EU.3.7.; H2020-EU.2.3.1.	Unmanned Aerial Vehicle for protecting soft/critical urban infrastructures, and the general public in extreme environments.	1/04/2016	31/07/2016	71 429	50 000	H2020-SMEINST-1-2015	ES		Critical infrastructures; Public spaces	Terrorism & radicalisation	UAV	YES
780355	FANDANGO	H2020-EU.2.1.1.	FAke News discovery and propagation from big Data ANalysis and artificial intelliGence Operations	1/01/2018	31/12/2020	3 583 125	2 879 250	H2020-ICT-2017-1	IT	EL;ES;BE;IE;IT	Hybrid threats		Social media; ICT	YES
780108	FENTEC	H2020-EU.3.7.4.; H2020-EU.2.1.1.	Functional Encryption Technologies	1/01/2018	31/12/2020	4 223 141	4 223 141	H2020-DS-LEIT-2017	ES	FI;SI;CH;FR;DE; BE;UK	Cybersecurity	Cybercrime	Cryptography	YES
740575	FIRE-IN	H2020-EU.3.7.6.; H2020-EU.3.7.2.; H2020-EU.3.7.3.; H2020-EU.3.7.1.; H2020-EU.3.7.7.; H2020-EU.3.7.8.; H2020-EU.3.7.5.	FIRE-IN - Fire and Rescue Innovation Network	1/05/2017	30/04/2022	3 496 241	3 496 241	H2020-SEC-2016-2017-1	FR	ES;IT;DE;PL;FR; CZ;SE;EL	Other		Rescue	NO
701306	FLAME	H2020-EU.1.3.2.	Fragility and Geopolitics in the Middle East and North Africa	1/09/2016	31/08/2018	172 800	172 800	H2020-MSCA-IF-2015	BE		Other		External security	NO
766719	FLASH	H2020-EU.1.2.1.	Far-infrared Lasers Assembled using Silicon Heterostructures	1/11/2017	31/10/2020	3 206 499	3 206 499	H2020-FETOPEN-1-2016-2017	IT	DE;CH;UK	Border control	Terrorism & radicalisation		YES

Project id	Project acronym	Programme	Project title	Start Date	End Date	Total Cost (€)	EC Max Contribution (€)	Call	Coordinator Country	Participant Countries	Building block(s)	Priority(ies)	Main focus(es)	Dual Use
653879	FLYSEC	H2020-EU.3.7.	Optimising time-to-FLY and enhancing airport SECurity	1/05/2015	30/04/2018	4 141 375	4 089 500	H2020-DRS-2014	EL	UK;IL;LU;DE;EL	Border control; Critical infrastructures	Terrorism & radicalisation	Biometrics; Surveillance	YES
682317	FOLLOW	H2020-EU.1.1.	Finance/Security practice after 9/11: Following the Money from Transaction to Trial	1/09/2016	31/08/2021	1 999 858	1 999 858	ERC-2015-CoG	NL		Terrorism financing	Terrorism & radicalisation; Organised crime		NO
653355	FORENSOR	H2020-EU.3.7.	FOREnsic evidence gathering autonomous seNSOR	1/09/2015	31/08/2018	4 937 834	4 043 546	H2020-FCT-2014	EL	BE;IL;EL;ES;IT;FR;PT	Other	Organised crime	Law enforcement; Surveillance ; Forensics	YES
740690	FORTIKA	H2020-EU.3.7.4.	FORTIKA - Cyber Security Accelerator for trusted SMEs IT Ecosystems	1/06/2017	31/05/2020	4 918 813	3 997 025	H2020-DS-SC7-2016	EL	UK;EL;ES;IT;SI;IE;DE;BG;BE	Cybersecurity	Cybercrime		YES
641492	FOSTER ITS	H2020-EU.2.1.6.	First Operational, Secured and Trusted galilEo Receiver for ITS	1/01/2015	31/12/2017	2 590 461	1 813 323	H2020-Galileo-2014-1	FR	DE;FR;IT	Space; Cybersecurity	Cybercrime	Applications in satellite navigation; Transport	YES
779391	FutureTPM	H2020-EU.3.7.4.; H2020-EU.2.1.1.	Future Proofing the Connected World: A Quantum-Resistant Trusted Platform Module	1/01/2018	31/12/2020	4 868 890	4 868 890	H2020-DS-LEIT-2017	AT	AT;CH;DE;UK;EL;LU;CY; IE;PT	Cybersecurity	Cybercrime	Cryptography	YES
700542	FutureTrust	H2020-EU.3.7.	Future Trust Services for Trustworthy Global Transactions	1/06/2016	31/05/2019	7 474 031	6 338 949	H2020-DS-2015-1	DE	BE;GE;UK;LU;ZA;TR;AT;PT;RS;DE	Cybersecurity	Cybercrime		YES
700670	GAP	H2020-EU.3.7.	Gaming for Peace	1/09/2016	28/02/2019	2 035 438	2 035 438	H2020-BES-2015	IE	PL;FI;IE;BG;NL;PT;UK	Defence		External security; Peace keeping; Training	YES
783183	GATEMAN	H2020-EU.3.4.7.	GNSS NAVIGATION THREATS MANAGEMENT	1/01/2018	31/12/2019	565 744	565 744	H2020-SESAR-2016-2	ES	FI;IT	Space; Cybersecurity	Cybercrime	Applications in satellite navigation; Transport	YES
776293	GAUSS	H2020-EU.3.4.2.2.; H2020-EU.3.4.1.2.; H2020-EU.2.1.6.3.; H2020-EU.2.1.6.1.2.	Galileo-EGNOS as an Asset for UTM Safety and Security	1/03/2018	28/02/2021	3 695 758	2 972 489	H2020-GALILEO-GSA-2017-1	ES	EL;IT;ES;NL;UK	Space		Applications in satellite navigation; UAV	YES
740923	GHOST	H2020-EU.3.7.4.	Safe-Guarding Home IoT Environments with Personalised Real-time Risk Control	1/05/2017	30/04/2020	4 995 519	3 603 832	H2020-DS-SC7-2016	ES	EL;NO;UK;CH;ES;DE	Cybersecurity	Cybercrime	IoT	YES
758834	GRIEVANCE	H2020-EU.1.1.	Gauging the Risk of Incidents of Extremist Violence Against Non-Combatant Entities	1/01/2018	31/12/2022	1 458 345	1 458 345	ERC-2017-STG	UK		Combating radicalisation	Terrorism & radicalisation	Social sciences; Violence	YES
683133	GROUPVIOLENCE	H2020-EU.1.1.	Groups and Violence: A Micro-sociological Research Programme	1/09/2016	31/08/2021	1 918 306	1 918 306	ERC-2015-CoG	NL		Combating radicalisation	Terrorism & radicalisation	Social sciences; Violence	NO
670172	GTCMR	H2020-EU.1.1.	Global Terrorism and Collective Moral Responsibility: Redesigning Military, Police and Intelligence Institutions in Liberal Democracies	1/01/2016	31/12/2020	2 479 810	2 479 810	ERC-2014-ADG	NL	UK	Combating radicalisation	Terrorism & radicalisation	Ethical dimension; Social sciences; Violence	YES
644052	HECTOR	H2020-EU.2.1.1.	HARDWARE ENABLED CRYPTO AND RANDOMNESS	1/03/2015	28/02/2018	4 494 088	4 494 088	H2020-ICT-2014-1	AT	AT;FR;NL;IT;BE;SK	Cybersecurity	Cybercrime	Cryptography; ICT	YES

Project id	Project acronym	Programme	Project title	Start Date	End Date	Total Cost (€)	EC Max Contribution (€)	Call	Coordinator Country	Participant Countries	Building block(s)	Priority(ies)	Main focus(es)	Dual Use
740689	HEIMDALL	H2020-EU.3.7.5.	HEIMDALL - MULTI-HAZARD COOPERATIVE MANAGEMENT TOOL FOR DATA EXCHANGE, RESPONSE PLANNING AND SCENARIO BUILDING	1/05/2017	31/10/2020	8 591 344	7 836 371	H2020-SEC-2016-2017-1	DE	IT;DK;ES;EL;FR;UK;DE	Public spaces; Critical infrastructures	Terrorism & radicalisation	Preparedness; Resilience; Disaster management	YES
740322	HERMENEUT	H2020-EU.3.7.4.	Enterprises intangible Risks Management via Economic models based on simulation of modern cyber-attacks	1/05/2017	30/04/2019	2 007 693	2 007 693	H2020-DS-SC7-2016	IT	UK;IT;FR;BE;IL;DE	Cybersecurity	Cybercrime	Social sciences	YES
756672	Human Trafficking	H2020-EU.1.1.	Human Trafficking: A Labor Perspective	1/04/2018	31/03/2023	1 492 250	1 492 250	ERC-2017-STG	IL		Other	Organised crime	Migration; Social sciences	NO
700626	iBorderCtrl	H2020-EU.3.7.	Intelligent Portable Border Control System	1/09/2016	31/08/2019	4 501 878	4 501 878	H2020-BES-2015	LU	ES;UK;HU;EL;LV;PL;CY;DE	Border control	Terrorism & radicalisation		YES
653909	ICT4COP	H2020-EU.3.7.	Community-Based Policing and Post-Conflict Police Reform	1/06/2015	31/05/2020	4 999 999	4 999 998	H2020-FCT-2014	NO	IE;UK;NO; DE;PL	Other	Organised crime	Law enforcement; Social sciences	NO
736454	IDAaaS	H2020-EU.3.7.; H2020-EU.2.3.1.	Trusted online service for identity assurance	1/10/2016	31/03/2017	71 429	50 000	H2020-SMEINST-1-2016-2017	NO		Cybersecurity	Cybercrime	Privacy	YES
690907	IDENTITY	H2020-EU.1.3.3.	Computer Vision Enabled Multimedia Forensics and People Identification	1/01/2016	31/12/2019	2 025 000	2 025 000	H2020-MSCA-RISE-2015	UK	SI;AT;IT;FR;ES	Other		Biometrics; Law enforcement; Forensics	YES
653371	IECEU	H2020-EU.3.7.	Improving the Effectiveness of the Capabilities (IEC) in EU conflict prevention	1/05/2015	31/01/2018	2 081 110	2 081 110	H2020-BES-2014	FI	NL;DK;FI;AT;IE;SI	Defence	Terrorism & radicalisation; Organised crime	External security	YES
740685	I-LEAD	H2020-EU.3.7.6; H2020-EU.3.7.2; H2020-EU.3.7.3; H2020-EU.3.7.1; H2020-EU.3.7.7; H2020-EU.3.7.8; H2020-EU.3.7.5.	Innovation - Law Enforcement Agencies Dialogue	1/09/2017	31/08/2022	3 483 718	3 483 716	H2020-SEC-2016-2017-1	NL	BE;RO;NL;IT;FR;PL;LT;PT;FI;EL;ES;UK	Other		Law enforcement	NO
740714	ILEAnet	H2020-EU.3.7.6; H2020-EU.3.7.2; H2020-EU.3.7.3; H2020-EU.3.7.1; H2020-EU.3.7.7; H2020-EU.3.7.8; H2020-EU.3.7.5.	Innovation by Law Enforcement Agencies networking	1/06/2017	31/05/2022	3 482 146	3 482 146	H2020-SEC-2016-2017-1	FR	CY;IE;FR;IT;RO;AT;SK;IL;HU;EE;ES;LV;UK;CZ;BG;PL;DE	Other		Law enforcement	NO
653383	IMPACT	H2020-EU.3.7.	Impact of Cultural aspects in the management of emergencies in public Transport	1/05/2015	31/10/2017	1 398 913	1 398 913	H2020-DRS-2014	IT	TR;NL;UK;IT;PL;BG	Public spaces	Terrorism & radicalisation	Emergency; Social sciences; Transport	YES
653390	IMPROVER	H2020-EU.3.7.	Improved risk evaluation and implementation of resilience concepts to critical infrastructure	1/06/2015	31/05/2018	4 323 979	4 323 979	H2020-DRS-2014	SE	NO;UK;DK;FR;PT;BE	Critical infrastructures	Terrorism & radicalisation	Resilience	YES
776487	INFACT	H2020-EU.3.5.3.	Innovative, Non-invasive and Fully Acceptable Exploration Technologies	1/11/2017	31/10/2020	5 624 030	5 624 030	H2020-SC5-2017-OneStageB	DE	ES;FI;DE;FR;IT;UK;ZA	Critical supplies		Supply security	YES

Project id	Project acronym	Programme	Project title	Start Date	End Date	Total Cost (€)	EC Max Contribution (€)	Call	Coordinator Country	Participant Countries	Building block(s)	Priority(ies)	Main focus(es)	Dual Use
740627	IN-PREP	H2020-EU.3.7.5.	An INtegrated next generation PREParedness programme for improving effective inter-organisational response capacity in complex environments of disasters and causes of crises	1/09/2017	31/08/2020	9 580 781	7 999 556	H2020-SEC-2016-2017-1	EL	IE;FR;IT;EL;DE;NL;UK	Critical infrastructures; Public spaces	Terrorism & radicalisation	Preparedness; Disaster management	YES
774928	iSAFE	H2020-EU.3.6.; H2020-EU.2.3.1.	iSAFE Internet Safety Awareness for European primary school children	1/06/2017	31/12/2017	71 429	50 000	H2020-SMEINST-1-2016-2017	IE		Cybersecurity	Cybercrime	Violence	YES
664639	KIOS	H2020-EU.4.a.	KIOS Research Center of Excellence for Intelligent Systems and Networks	1/06/2015	31/05/2016	417 000	417 000	H2020-WIDESPREAD-2014-1	CY	UK	Critical infrastructures	Terrorism & radicalisation	ICT	YES
739551	KIOS CoE	H2020-EU.4.a.	KIOS Research and Innovation Centre of Excellence	1/03/2017	29/02/2024	15 000 000	15 000 000	H2020-WIDESPREAD-01-2016-2017-TeamingPhase2	CY	UK	Critical infrastructures	Terrorism & radicalisation	ICT	YES
727528	KONFIDO	H2020-EU.3.7.4.; H2020-EU.3.1.	KONFIDO - Secure and Trusted Paradigm for Interoperable eHealth Services	1/11/2016	31/10/2019	4 992 078	4 992 078	H2020-DS-SC1-2016	UK	IT;BE;EL;UK;DK;FR;ES	Cybersecurity	Cybercrime	Privacy	YES
653587	LAW-TRAIN	H2020-EU.3.7.	Mixed-reality environment for training teams in joint investigative interrogation-Intelligent interrogation training simulator	1/05/2015	30/04/2018	5 095 688	5 095 687	H2020-FCT-2014	IL	AT;ES;RO;IL;PT;BE	Other	Organised crime	Law enforcement	NO
740466	LETS-CROWD	H2020-EU.3.7.6.; H2020-EU.3.7.1.	Law Enforcement agencies human factor methods and Toolkit for the Security and protection of CROWDs in mass gatherings	1/05/2017	31/10/2019	2 919 308	2 919 308	H2020-SEC-2016-2017-1	ES	DE;UK;BE;ES;IT;RO;IL;PT	Public spaces	Terrorism & radicalisation; Organised crime	Law enforcement	YES
727982	LINCOLN	H2020-EU.3.2.5.	Lean innovative connected vessels	1/10/2016	30/09/2019	7 808 691	6 343 600	H2020-BG-2016-1	IT	NO;ES;IT;DE;CY;EL	Other		Emergency; Rescue; IoT	YES
761947	LocationWise	H2020-EU.3.7.; H2020-EU.2.3.1.	LocationWise Payment Card Validation: A cloud based location verification system that willsignificantly lower cost of payment card cyber security	1/03/2017	31/08/2017	71 429	50 000	H2020-SMEINST-1-2016-2017	UK		Cybersecurity	Cybercrime		YES
661362	LV-Pri20	H2020-EU.1.3.2.	Logic-based Verification of Privacy-Preservation in Europe's 2020 ICT	22/06/2015	21/06/2017	195 455	195 455	H2020-MSCA-IF-2014	UK	UK	Cybersecurity	Cybercrime	Privacy; IoT	YES
752144	MAPS	H2020-EU.1.3.2.	MAPS – Migrants And People Smugglers: A Comparative Study of Smuggling Networks in the Eastern Mediterranean and the Central American corridors	1/09/2017	31/08/2020	262 269	262 269	H2020-MSCA-IF-2016	IT		Border control	Organised crime	Migration; Social sciences	NO
653004	MARGIN	H2020-EU.3.7.	Tackle Insecurity in Marginalized Areas	1/05/2015	30/04/2017	1 881 400	1 881 400	H2020-FCT-2014	ES	ES;FR;HU;IT;UK	Other		Social sciences	NO
740698	MARISA	H2020-EU.3.7.3.; H2020-EU.3.7.7.	Maritime Integrated Surveillance Awareness	1/05/2017	31/10/2019	9 765 659	7 997 493	H2020-SEC-2016-2017-1	IT	IT;FI;NL;EL;DE;BE;FR; PT;ES	Border control	Organised crime; Terrorism & radicalisation	Migration; Surveillance	YES
700281	MEDIA4SEC	H2020-EU.3.7.	The emerging role of new social media in enhancing public security	1/07/2016	31/12/2018	1 917 006	1 902 006	H2020-FCT-2015	UK	NL;SI;DE;ES;FR;BE;EL;UK	Cybersecurity; Combating radicalisation	Terrorism & radicalisation; Cybercrime	Social media	YES

Project id	Project acronym	Programme	Project title	Start Date	End Date	Total Cost (€)	EC Max Contribution (€)	Call	Coordinator Country	Participant Countries	Building block(s)	Priority(ies)	Main focus(es)	Dual Use
653626	microMole	H2020-EU.3.7.	SEWAGE MONITORING SYSTEM FOR TRACKING SYNTHETIC DRUG LABORATORIES	1/09/2015	31/08/2018	5 451 388	4 992 866	H2020-FCT-2014	PL	FR;BE;DE; SE;IS;NL;PL	Other	Organised crime	Law enforcement; Forensics	YES
740543	MINDb4ACT	H2020-EU.3.7.6.; H2020-EU.3.7.1.	Mapping, IdentifiNg and Developing skills and opportunities in operating environments to co-create innovative, ethical and effective ACTions to tackle radicalization leading to violent extremism	1/09/2017	31/08/2020	2 999 310	2 999 310	H2020-SEC-2016-2017-1	ES	DE;FR;IT;AT;PL; BE;DK; ES;UK;FI	Combating radicalisation	Terrorism & radicalisation	Migration; Social media; Violence	NO
653212	MITIGATE	H2020-EU.3.7.	Multidimensional, IntegraTed, risk assessment framework and dynamic, collaborative Risk ManaGement tools for critical information infrAstrucTurEs	1/09/2015	28/02/2018	3 549 869	3 109 795	H2020-DS-2014-1	DE	UK;AT;RO; ES;IT;EL;DE	Cybersecurity; Critical infrastructures	Cybercrime	Supply chain; transport	YES
687338	MOBNET	H2020-EU.2.1.6.	MOBile NETwork for people's location in natural and man-made disasters	1/01/2016	28/02/2018	1 242 534	986 272	H2020-Galileo-2015-1	ES	DE;PL;NL;ES	Space; Public spaces	Terrorism & radicalisation	Applications in satellite navigation; Rescue; UAV	YES
644429	MUSA	H2020-EU.2.1.1.3.	MULTi-cloud Secure Applications	1/01/2015	31/12/2017	3 574 190	3 574 190	H2020-ICT-2014-1	ES	DE;FI;IT;UK;FR; ES	Cybersecurity	Cybercrime	Cloud; ICT	YES
703071	MUSLIM-NLNO	H2020-EU.1.3.2.	Muslims condemning violent extremism - An interdisciplinary analysis of public initiatives in the Netherlands and Norway 2001-2015	1/06/2016	31/05/2018	177 599	177 599	H2020-MSCA-IF-2015	NL		Combating radicalisation	Terrorism & radicalisation	Social sciences	NO
707482	MWDIR	H2020-EU.1.3.2.	Media Warfare and the Discourse of Islamic Revival: The Case of the Islamic State (IS)	1/02/2017	31/01/2019	195 455	195 455	H2020-MSCA-IF-2015	UK		Combating radicalisation	Terrorism & radicalisation	Social media; Social sciences	NO
754682	NANOELECTR OCHEM	H2020-EU.1.1.	Electrocatalytic Nanoreactors for Absorption, Detection and Decontamination of Hazardous Compounds	1/12/2017	31/05/2019	149 912	149 912	ERC-2016-PoC	UK		CBRN-E	Terrorism & radicalisation		YES
675320	NeCS	H2020-EU.1.3.1.	European Network for Cyber-security	1/09/2015	31/08/2019	3 882 228	3 882 228	H2020-MSCA-ITN-2015	IT	ES;UK;IT;DE	Cybersecurity	Cybercrime	Preparedness; Training	YES
653839	NOSY	H2020-EU.3.7.	New Operational Sensing sYstem	1/09/2015	31/08/2018	5 389 133	4 198 685	H2020-FCT-2014	IT	IT;PT;SE;UK;FR	Other	Organised crime	Law enforcement; Forensics	YES
748164	NWICWEP	H2020-EU.1.3.2.	NON-WESTERN MILITARY INTERVENTIONS AND THE CHARACTER OF WARFARE IN THE EUROPEAN PERIPHERY	1/09/2018	31/08/2020	180 277	180 277	H2020-MSCA-IF-2016	IT		Defence		Social sciences; External security	YES
705207	OCGN	H2020-EU.1.3.2.	Traditional Organised Crime and the Internet: The changing organization of illegal gambling networks	22/05/2017	21/11/2018	146 591	146 591	H2020-MSCA-IF-2015	UK		Cybersecurity	Organised crime; Cybercrime	Social sciences	YES
647850	OCTAVE	H2020-EU.3.7.	Objective Control for TAlker VErification	1/06/2015	31/07/2017	5 208 985	4 406 116	H2020-DS-2014-1	IT	IT;UK;FI;EL;ES; FR;DK	Cybersecurity	Cybercrime	Biometrics	YES
703225	OHS	H2020-EU.1.3.2.	On Human Shielding	1/09/2017	31/08/2019	195 455	195 455	H2020-MSCA-IF-2015	UK		Defence		Social sciences; External security; Violence	NO
653704	OPERANDO	H2020-EU.3.7.	Online Privacy Enforcement, Rights Assurance and Optimization	42125	43220	4 455 811	3 746 037	H2020-DS-2014-1	UK	IT;RO;ES; DE;EL;UK;IL	Cybersecurity	Cybercrime	Privacy	YES

Project id	Project acronym	Programme	Project title	Start Date	End Date	Total Cost (€)	EC Max Contribution (€)	Call	Coordinator Country	Participant Countries	Building block(s)	Priority(ies)	Main focus(es)	Dual Use
644814	PaaSword	H2020-EU.2.1.1.3.	A Holistic Data Privacy and Security by Design Platform-as-a-Service Framework Introducing Distributed Encrypted Persistence in Cloud-based Applications	1/01/2015	31/12/2017	4 461 513	3 984 575	H2020-ICT-2014-1	DE	EL;CH;RO;SE;DE;CY;LU	Cybersecurity	Cybercrime	Cryptography; Cloud; ICT	YES
653497	PANORAMIX	H2020-EU.3.7.	Privacy and Accountability in Networks via Optimized Randomized Mix-nets	42248	43496	4 459 711	3 796 625	H2020-DS-2014-1	UK	NL;EE;EL;DE;BE;UK	Cybersecurity	Cybercrime	Privacy	YES
700583	PeaceTraining.eu	H2020-EU.3.7.	Strengthening the Capabilities and Training Curricula for Conflict Prevention and Peace Building Personnel with ICT-based Collaboration and Knowledge Approaches	1/09/2016	31/10/2018	1 499 920	1 499 920	H2020-BES-2015	AT	DE;UK;AT;XK;EE;RO;ES;BE	Defence		External security; Peace keeping; Training	YES
740773	Pericles	H2020-EU.3.7.6.; H2020-EU.3.7.1.	Policy recommendation and improved communication tools for law enforcement and security agencies preventing violent radicalisation	1/05/2017	30/04/2020	2 999 648	2 999 648	H2020-SEC-2016-2017-1	DE	FR;IE;NL;ES;EL;UK;DE;BA	Combating radicalisation	Terrorism & radicalisation	Law enforcement; Violence	YES
677595	POLICIES_FOR_PEACE	H2020-EU.1.1.	The economics of lasting peace: The role of policies and institutions	1/08/2016	31/07/2021	1 013 720	1 013 720	ERC-2015-STG	CH		Other		Social sciences; External security; Peace keeping	NO
708815	POMEGRANATE	H2020-EU.1.3.2.	Practice-Oriented Security Models and Granular Designs for Future-Proof Authenticated Encryption	1/09/2017	30/08/2020	172 800	172 800	H2020-MSCA-IF-2015	BE		Cybersecurity	Cybercrime	Cryptography; IoT; Cloud	YES
714955	POPSTAR	H2020-EU.1.1.	Reasoning about Physical properties Of security Protocols with an Application To contactless Systems	1/02/2017	31/01/2022	1 499 750	1 499 750	ERC-2016-STG	FR		Cybersecurity	Cybercrime	Cryptography	YES
645622	PQCRYPTO	H2020-EU.2.1.1.	Post-quantum cryptography for long-term security	1/03/2015	28/02/2018	3 964 791	3 851 791	H2020-ICT-2014-1	NL	FR;IL;NL;DE;BE;DK;TW	Cybersecurity	Cybercrime	Cryptography; IoT; Cloud; ICT	YES
740072	PRACTICES	H2020-EU.3.7.6.; H2020-EU.3.7.1.	Partnership against violent radicalization in the cities	1/05/2017	30/04/2020	3 378 970	3 378 970	H2020-SEC-2016-2017-1	FR	TN;FR;AT;BE;ES;PT;EL;IT	Combating radicalisation	Terrorism & radicalisation	Social media; Social sciences	YES
644962	PRISMACLOUD	H2020-EU.2.1.1.	PRivacy and Security MAintaining services in the CLOUD	1/02/2015	31/07/2018	8 381 953	7 983 009	H2020-ICT-2014-1	AT	AT;CH;FR;UK;DE;IT;ES;IL;SE	Cybersecurity	Cybercrime	Privacy; Cloud; ICT	YES
653426	PRIVACY FLAG	H2020-EU.3.7.	Enabling Crowd-sourcing based privacy protection for smartphone applications, websites and Internet of Things deployments	1/05/2015	30/04/2018	4 538 438	3 143 000	H2020-DS-2014-1	EL	SE;EL;DK;RS;IT;LU;CH;UK	Cybersecurity	Cybercrime	Privacy	YES
780477	PRIViLEDGE	H2020-EU.3.7.4.; H2020-EU.2.1.1.	Privacy-Enhancing Cryptography in Distributed Ledgers	1/01/2018	31/12/2020	4 527 918	4 527 918	H2020-DS-LEIT-2017	EE	EL;IT;EE;CH;NL;UK	Cybersecurity	Cybercrime	Privacy; Cryptography; Blockchain	YES
780701	PROMETHEUS	H2020-EU.3.7.4.; H2020-EU.2.1.1.	PRivacy preserving pOst-quantuM systEmS from advanced cryptOgrapHic mEchanisms Using latticeS	1/01/2018	31/12/2021	5 496 969	5 496 969	H2020-DS-LEIT-2017	FR	FR;NL;IL;ES;CH;DE;UK	Cybersecurity	Cybercrime	Privacy; Cryptography	YES
690972	PROTASIS	H2020-EU.1.3.3.	Restoring Trust in the cyber space: a Systems Security Proposal	1/05/2016	30/04/2020	702 000	702 000	H2020-MSCA-RISE-2015	EL	NL;ES;DE;IT;FI	Cybersecurity	Cybercrime		YES
700259	PROTECT	H2020-EU.3.7.	Pervasive and UseR Focused BiomeTrics BordEr ProjeCT	1/09/2016	31/08/2019	4 981 753	4 981 753	H2020-BES-2015	UK	DE;AT;PL;FR;UK;BE	Border control	Terrorism & radicalisation; Organised crime	Biometrics	YES

Project id	Project acronym	Programme	Project title	Start Date	End Date	Total Cost (€)	EC Max Contribution (€)	Call	Coordinator Country	Participant Countries	Building block(s)	Priority(ies)	Main focus(es)	Dual Use
700071	PROTECTIVE	H2020-EU.3.7.	Proactive Risk Management through Improved Cyber Situational Awareness	1/09/2016	31/08/2019	4 693 613	4 160 597	H2020-DS-2015-1	IE	CZ;ES;AT;PL;IE;DE;UK;RO	Cybersecurity	Cybercrime	Preparedness	YES
699824	PROTON	H2020-EU.3.7.	Modelling the PRocesses leading to Organised crime and TerrOrist Networks	1/10/2016	30/09/2019	4 464 507	4 094 812	H2020-FCT-2015	IT	BE;DE;US;UK;NL;IT;CH;ES;PL;IL;SE	Combating radicalisation; Cybersecurity	Terrorism & radicalisation; Cybercrime	Social sciences	NO
714294	QUASYModo	H2020-EU.1.1.	Symmetric Cryptography in the Post-Quantum World	1/09/2017	31/08/2022	1 330 463	1 330 463	ERC-2016-STG	FR		Cybersecurity	Cybercrime	Cryptography	YES
700326	RAMSES	H2020-EU.3.7.	Internet Forensic platform for tracking the money flow of financially-motivated malware	1/09/2016	31/08/2019	3 803 088	3 532 000	H2020-FCT-2015	ES	DE;BE;IT;PT;ES;UK	Cybersecurity; Terrorism financing	Cybercrime	Law enforcement; Forensics	YES
756482	REACT	H2020-EU.1.1.	Realizable Advanced Cryptography	1/10/2017	30/09/2022	1 493 803	1 493 803	ERC-2017-STG	IL		Cybersecurity	Cybercrime	Cryptography	YES
731591	REASSURE	H2020-EU.3.7.; H2020-EU.2.1.1.	Robust and Efficient Approaches to Evaluating Side Channel and Fault Attack Resilience	1/01/2017	31/12/2019	3 528 635	3 478 748	H2020-DS-LEIT-2016	BE	FR;DE;NL;UK	Cybersecurity	Cybercrime	Certification; IoT	YES
740688	RED-Alert	H2020-EU.3.7.6.; H2020-EU.3.7.1.	Real-time Early Detection and Alert System for Online Terrorist Content based on Natural Language Processing, Social Network Analysis, Artificial Intelligence and Complex Event Processing	1/06/2017	31/05/2020	5 064 438	5 064 438	H2020-SEC-2016-2017-1	RO	RO;UK;IL;MD;HU;ES;MT;FR	Other	Terrorism & radicalisation	Law enforcement; Social media	YES
775251	REDSENTRY	H2020-EU.3.7.; H2020-EU.2.3.1.	Proactive Operational Intelligence Cybersecurity Platform for the Financial Services Industry	1/07/2017	31/12/2017	71 429	50 000	H2020-SMEINST-1-2016-2017	ES		Cybersecurity	Cybercrime		YES
792793	REJREG	H2020-EU.1.3.2.	Rejection Regimes: An Ethnographic Study of the Social Life of Intra-EU Border Regimes	1/04/2018	31/03/2020	165 599	165 599	H2020-MSCA-IF-2017	NL		Border control		Migration; Social sciences	NO
653260	RESILENS	H2020-EU.3.7.	RESILENS: Realising European ReSilience for Critical INfraStructure	1/05/2015	30/04/2018	4 091 843	4 091 843	H2020-DRS-2014	IE	PT;IE;DE;IL;UK	Critical infrastructures	Terrorism & radicalisation	Resilience	YES
700389	ResiStand	H2020-EU.3.7.	Increasing disaster Resilience by establishing a sustainable process to support Standardisation of technologies and services	1/05/2016	30/04/2018	1 962 554	1 962 554	H2020-DRS-2015	FI	NL;ES;FI;DE;IT;NO;UK	Other	Terrorism & radicalisation	Resilience; Standardisation; Disaster management	YES
653460	RESOLUTE	H2020-EU.3.7.	RESilience management guidelines and Operationalization applIed to Urban Transport Environment	1/05/2015	30/04/2018	3 848 581	3 848 581	H2020-DRS-2014	IT	IT;EL;DE;PT;FR	Critical infrastructures	Terrorism & radicalisation	Resilience; Transport	YES
731678	RESTASSURED	H2020-EU.2.1.1.	Secure Data Processing in the Cloud	1/01/2017	31/12/2019	4 996 299	4 996 297	H2020-ICT-2016-1	IL	FR;DE;UK	Cybersecurity	Cybercrime	Cloud; ICT	YES
673801	ROBIN	H2020-EU.3.7.; H2020-EU.2.3.1.	ROBotic security INnovative system	1/07/2015	31/12/2015	71 429	50 000	H2020-SMEINST-1-2014	ES		Critical infrastructures	Terrorism & radicalisation		YES
740593	ROBORDER	H2020-EU.3.7.3.; H2020-EU.3.7.7.	autonomous swarm of heterogeneous RObots for BORDER surveillance	1/05/2017	30/04/2020	8 997 782	7 999 316	H2020-SEC-2016-2017-1	PT	RO;ES;CH;EL;FI;BG;DE;IT;PT;BE;EE;UK;HU	Border control	Organised crime; Terrorism & radicalisation	Surveillance	YES

Project id	Project acronym	Programme	Project title	Start Date	End Date	Total Cost (€)	EC Max Contribution (€)	Call	Coordinator Country	Participant Countries	Building block(s)	Priority(ies)	Main focus(es)	Dual Use
700264	ROCSAFE	H2020-EU.3.7.	Remotely Operated CBRNe Scene Assessment Forensic Examination	1/07/2016	30/06/2019	4 781 061	4 781 061	H2020-FCT-2015	IE	ES;IT;IE;DE;PT	CBRN-E		Law enforcement; Forensics	YES
653884	SafeCloud	H2020-EU.3.7.	Secure and Resilient Cloud Architecture	1/09/2015	31/08/2018	3 298 988	2 150 810	H2020-DS-2014-1	PT	EE;DE;CH;PT	Cybersecurity	Cybercrime	Privacy; Cloud	YES
644729	SAFEcrypto	H2020-EU.2.1.1.	Secure Architectures of Future Emerging Cryptography	1/01/2015	31/12/2018	4 081 827	3 266 927	H2020-ICT-2014-1	UK	FR;CH;UK;DE;IE	Cybersecurity	Cybercrime	Cryptography; ICT	YES
700643	SafeShore	H2020-EU.3.7.	System for detection of Threat Agents in Maritime Border Environment	1/05/2016	31/10/2018	5 133 583	5 133 583	H2020-BES-2015	BE	RO;CZ;BE; BG;IL;UK;IT	Border control	Organised crime	Surveillance	YES
644080	SAFURE	H2020-EU.2.1.1.1.	SAFeTy and secURity by design for interconnected mixed-critical cyber-physical systems	1/02/2015	31/01/2018	5 702 631	5 231 375	H2020-ICT-2014-1	AT	FR;DE;IT;CH;AT;ES	Cybersecurity	Cybercrime	CPS; ICT	YES
776099	SARA	H2020-EU.3.2.1.; H2020-EU.2.1.6.3.; H2020-EU.2.1.6.1.2.	Search And Rescue Aid and Surveillance using High EGNSS Accuracy	1/02/2018	31/01/2020	1 942 328	1 455 583	H2020-GALILEO-GSA-2017-1	IT	DK;IT;BE;NL;PL	Border control; Space		Migration; Rescue; Surveillance; Applications in satellite navigation; UAV	YES
740477	SAURON	H2020-EU.3.7.4.; H2020-EU.3.7.2.	Scalable multidimensionAl sitUation awaReness sOlution for protectiNg european ports	1/05/2017	30/04/2020	8 491 173	6 926 370	CIP-2016-2017-1	ES	FR;UK;AT;IT;SI; EL;ES;BE	Critical infrastructures; Hybrid threats; Cybersecurity	Terrorism & radicalisation; Cybercrime	Physical threats	YES
644425	SCISSOR	H2020-EU.2.1.1.	Security In trusted SCADA and smart-grids	1/01/2015	31/12/2017	3 989 850	3 534 850	H2020-ICT-2014-1	FR	FR;CH;PL;IT;AT; BE	Cybersecurity; Critical infrastructures	Cybercrime	ICT	YES
777996	SealedGRID	H2020-EU.1.3.3.	Scalable, trustEd, and interoperAble pLatform for sECureD smart GRID	1/01/2018	31/12/2021	1 080 000	1 080 000	H2020-MSCA-RISE-2017	EL	RO;ES;EL	Critical infrastructures; Cybersecurity	Cybercrime	Physical threats	YES
763599	SECOPS	H2020-EU.3.4.7.	An Integrated Security Concept for Drone Operations	1/10/2017	30/09/2019	909 294	909 294	H2020-SESAR-2016-1	NL	FI;BE;NL	Other		UAV	YES
736395	SecTrap	H2020-EU.3.7.; H2020-EU.2.3.1.	Critical urban infrastructure and soft target cyber attack protection. Users and application Behavioural Analysis supported by artificial intelligence to preempt security cyber attacks.	1/09/2016	28/02/2017	71 429	50 000	H2020-SMEINST-1-2016-2017	PT		Critical infrastructures; Public spaces; Cybersecurity	Cybercrime		YES
779899	SecureIoT	H2020-EU.2.1.1.	Predictive Security for IoT Platforms and Networks of Smart Objects	1/01/2018	31/12/2020	4 860 335	4 860 335	H2020-IOT-2017	BE	FR;DE;NL; RO;EL;ES; CY;BE;LU	Cybersecurity	Cybercrime	IoT	YES
645114	SEERS	H2020-EU.2.1.1.6.	Snapshot spEctral imagEr for cost effective IR Surveillance	1/02/2015	31/01/2018	3 750 535	3 750 535	H2020-ICT-2014-1	ES	NL;ES;IT;FR;TR; UK	Other		ICT; Surveillance	YES
645011	SERECa	H2020-EU.2.1.1.3.	Secure Enclaves for REactive Cloud Applications	1/03/2015	28/02/2018	3 834 340	3 834 340	H2020-ICT-2014-1	DE	UK;DE;IT;IE	Cybersecurity; Critical infrastructures	Cybercrime	CPS; IoT; Cloud; ICT	YES
653450	SEREN 3	H2020-EU.3.7.	Security Research NCP Network 3	1/05/2015	30/04/2018	1 995 451	1 995 451	H2020-DRS-2014	IT	LV;ES;EE;IS;BE; CY;TR;SK;EL;PL; IL;ZA; HR;RO;CZ	Other		Information exchange	NO

Project id	Project acronym	Programme	Project title	Start Date	End Date	Total Cost (€)	EC Max Contribution (€)	Call	Coordinator Country	Participant Countries	Building block(s)	Priority(ies)	Main focus(es)	Dual Use
780139	SerIoT	H2020-EU.2.1.1.	Secure and Safe Internet of Things	1/01/2018	31/12/2020	4 999 084	4 999 084	H2020-IOT-2017	PL	CY;EL;ES;AT;DE;UK;BE	Cybersecurity	Cybercrime	IoT	YES
682451	SEXHUM	H2020-EU.1.1.	Sexual Humanitarianism: understanding agency and exploitation in the global sex industry	1/10/2016	30/09/2020	1 600 000	1 600 000	ERC-2015-CoG	UK	FR	Border control	Organised crime	Migration; Social sciences	NO
734035	ShamROCK	H2020-EU.3.7.; H2020-EU.2.3.1.	ShamROCK – Secure professional Mobile Radio Over Commercial networkS	1/09/2016	31/10/2018	1 835 445	1 284 812	H2020-SMEINST-2-2016-2017	ES		Other		Emergency	YES
663021	ShamROCK	H2020-EU.3.7.; H2020-EU.2.3.1.	ShamROCK – Secure professional Mobile Radio Over Commercial networkS	1/02/2015	31/07/2015	71 429	50 000	H2020-SMEINST-1-2014	ES		Other		Emergency	YES
644571	SHARCS	H2020-EU.2.1.1.	Secure Hardware-Software Architectures for Robust Computing Systems	1/01/2015	31/12/2017	3 105 763	3 105 763	H2020-ICT-2014-1	EL	NL;DE;GI;IL;SE	Cybersecurity	Cybercrime	ICT	YES
727301	SHIELD	H2020-EU.3.7.4.; H2020-EU.3.1.	European Security in Health Data Exchange	1/01/2017	31/12/2019	3 897 268	3 897 268	H2020-DS-SC1-2016	ES	UK;ES;DE;IT;IL	Cybersecurity	Cybercrime	Privacy	YES
700199	SHIELD	H2020-EU.3.7.	Securing against intruders and other threats through a NFV-enabled environment	1/09/2016	28/02/2019	4 552 061	3 607 245	H2020-DS-2015-1	EL	EL;IT;ES;UK;LU;PT	Cybersecurity	Cybercrime		YES
778550	Signa2.0	H2020-EU.3.7.; H2020-EU.2.3.1.	Signaturit	1/01/2018	30/06/2019	1 739 188	1 217 431	H2020-SMEINST-2-2016-2017	ES		Cybersecurity	Cybercrime	Biometrics; Blockchain	YES
700621	SmartResilience	H2020-EU.3.7.	Smart Resilience Indicators for Smart Critical Infrastructures	1/05/2016	30/04/2019	4 960 831	4 809 949	H2020-DRS-2015	DE	RS;AT;IE;SE;EL;DE;NO;HU;FI;UK;CH;IL	Critical infrastructures	Terrorism & radicalisation	Resilience	YES
740787	SMESEC	H2020-EU.3.7.4.	Protecting Small and Medium-sized Enterprises digital technology through an innovative cyber-SECurity framework	1/06/2017	31/05/2020	5 683 820	3 998 922	H2020-DS-SC7-2016	ES	RO;CH;FR;ES;EL;NL;IL	Cybersecurity	Cybercrime		YES
740931	SMILE	H2020-EU.3.7.3.; H2020-EU.3.7.7.	SMart mobLiLity at the European land borders	1/07/2017	30/06/2020	4 999 276	4 999 276	H2020-SEC-2016-2017-1	EL	RO;UK;DE;EL;FR;BG;NO;HU	Border control	Terrorism & radicalisation; Organised crime	Biometrics; Cloud	YES
653569	SMR	H2020-EU.3.7.	Smart Mature Resilience	1/06/2015	31/05/2018	4 641 233	4 641 233	H2020-DRS-2014	ES	SE;IT;UK;NO;LV;DE;DK;ES	Critical infrastructures	Terrorism & radicalisation	Resilience	YES
705020	SOLOMON	H2020-EU.1.3.2.	Self-Organisation and Learning Online in Mobile Observation Networks	1/02/2017	31/01/2019	195 455	195 455	H2020-MSCA-IF-2015	UK		Public spaces	Terrorism & radicalisation	Law enforcement	YES
681402	SOPHIA	H2020-EU.1.1.	Securing Software against Physical Attacks	1/09/2016	31/08/2021	1 964 750	1 964 750	ERC-2015-CoG	AT		Cybersecurity	Cybercrime	Cryptography; Physical threats	YES
653586	SpeechXRays	H2020-EU.3.7.	Multi-channel biometrics combining acoustic and machine vision analysis of speech, lip movement and face	1/05/2015	30/04/2018	5 343 606	4 102 467	H2020-DS-2014-1	FR	UK;EE;EL;FR;RO	Cybersecurity	Cybercrime	Biometrics	YES

Project id	Project acronym	Programme	Project title	Start Date	End Date	Total Cost (€)	EC Max Contribution (€)	Call	Coordinator Country	Participant Countries	Building block(s)	Priority(ies)	Main focus(es)	Dual Use
645865	SPOOC	H2020-EU.1.1.	Automated Security Proofs of Cryptographic Protocols: Privacy, Untrusted Platforms and Applications to E-voting Protocols	1/09/2015	31/08/2020	1 903 500	1 903 500	ERC-2014-CoG	FR		Cybersecurity	Cybercrime	Privacy; Cryptography	YES
641486	spyGLASS	H2020-EU.2.1.6.	GALILEO-BASED PASSIVE RADAR SYSTEM FOR MARITIME SURVEILLANCE	1/01/2015	31/12/2017	1 510 250	1 069 317	H2020-Galileo-2014-1	IT	UK;DE;IT	Space	Organised crime	Applications in satellite navigation; Surveillance	YES
780439	StandICT.eu	H2020-EU.2.1.1.	Supporting European Experts Presence in International Standardisation Activities in ICT	1/01/2018	31/12/2019	2 000 000	2 000 000	H2020-ICT-2017-1	UK	DE	Cybersecurity	Cybercrime	Standardisation; ICT	NO
740610	STOP-IT	H2020-EU.3.7.4.; H2020-EU.3.7.2.	Strategic, Tactical, Operational Protection of water Infrastructure against cyber-physical Threats	1/06/2017	31/05/2021	9 616 525	8 255 320	CIP-2016-2017-1	NO	NO;NL;DE; ES;BE;IL;EL	Critical infrastructures; Cybersecurity	Cybercrime	CPS; Physical threats	YES
773932	STORM	H2020-EU.3.7.; H2020-EU.2.3.1.	The first cybersecurity management system providing evidence based metrics for cyber risk at the business asset level in real-time	1/07/2017	31/10/2017	71 429	50 000	H2020-SMEINST-1-2016-2017	IL		Cybersecurity	Cybercrime		NO
689364	STRADE	H2020-EU.3.5.3.	Strategic Dialogue on Sustainable Raw Materials for Europe	1/12/2015	30/11/2018	1 977 509	1 977 509	H2020-SC5-2015-one-stage	DE	UK;ZA;DE;SE	Critical supplies		Supply security	YES
700416	SUCCESS	H2020-EU.3.7.	Securing Critical Energy InfrastructuresSUCCESS - Securing Critical Energy Infrastructures	1/05/2016	31/10/2018	4 999 946	4 999 946	H2020-DRS-2015	DE	DE;IE;SE;NL;BE; EL;RO;IT;FI	Critical infrastructures; Cybersecurity	Cybercrime	CPS; Physical threats	YES
644666	SUNFISH	H2020-EU.2.1.1.3.	SecUre iNformation SHaring in federated heterogeneous private clouds	1/01/2015	31/12/2017	4 520 048	4 520 029	H2020-ICT-2014-1	IT	UK;AT;EE; MT;IL;IT	Cybersecurity	Cybercrime	Cloud; ICT	YES
643964	SUPERCLOUD	H2020-EU.2.1.1.3.	USER-CENTRIC MANAGEMENT OF SECURITY AND DEPENDABILITY IN CLOUDS OF CLOUDS	1/02/2015	31/01/2018	6 863 279	5 398 280	H2020-ICT-2014-1	AT	PT;FR;CH;NL;DE	Cybersecurity	Cybercrime	Cloud; ICT	YES
720417	SURVANT	H2020-EU.3.; H2020-EU.2.	SURveillance Video Archives iNvestigation assisTant	1/01/2017	31/12/2018	2 578 960	1 994 797	H2020-FTIPilot-2015-1	IT	EL;IT;ES;IE	Other		Law enforcement; Surveillance	YES
700688	TAKEDOWN	H2020-EU.3.7.	Understand the Dimensions of Organised Crime and Terrorist Networks for Developing Effective and Efficient Security Solutions for First-line-practitioners and Professionals	1/09/2016	31/08/2019	3 421 063	3 146 375	H2020-FCT-2015	AT	AT;ES;IT;UK;BG; CH;CZ; PL;RO;DE; SK;IL;BE	Other	Terrorism & radicalisation; Organised crime	Law enforcement; Social sciences	NO
653350	TARGET	H2020-EU.3.7.	Training Augmented Reality Generalised Environment Toolkit	1/05/2015	31/10/2018	5 992 360	5 992 360	H2020-FCT-2014	FR	AT;FR;NO; UK;DE;LU; ES;EE;NL;SK	Other	Terrorism & radicalisation; Cybersecurity	Law enforcement; Training	YES
700024	TENSOR	H2020-EU.3.7.	Retrieval and Analysis of Heterogeneous Online Content for Terrorist Activity Recognition	1/09/2016	31/08/2019	5 618 028	4 977 201	H2020-FCT-2015	UK	UK;ES;DE; BE;EL;FR;IT	Combating radicalisation	Terrorism & radicalisation; Organised crime	Law enforcement	YES
781623	TFence	H2020-EU.3.7.; H2020-EU.2.3.1.	A patent pending solution/microchip for the IoT cybersecurity market requirements: no access toonline software updates, very small size, inexpensive hardware, low energy consumption.	1/08/2017	30/11/2017	71 429	50 000	H2020-SMEINST-1-2016-2017	IL		Cybersecurity	Cybercrime	IoT	YES
740558	TITANIUM	H2020-EU.3.7.6.; H2020-EU.3.7.1.	Tools for the Investigation of Transactions in Underground Markets	1/05/2017	30/04/2020	4 991 600	4 991 600	H2020-SEC-2016-2017-1	AT	FR;NL;AT; ES;DE;UK;FI	Cybersecurity; Terrorism financing	Cybercrime; Organised crime	Law enforcement	YES

Project id	Project acronym	Programme	Project title	Start Date	End Date	Total Cost (€)	EC Max Contribution (€)	Call	Coordinator Country	Participant Countries	Building block(s)	Priority(ies)	Main focus(es)	Dual Use
682815	TOCNeT	H2020-EU.1.1.	Teaching Old Crypto New Tricks	1/04/2016	31/03/2021	1 882 244	1 882 244	ERC-2015-CoG	AT		Cybersecurity	Cybercrime	Cryptography	YES
653409	TOXI-triage	H2020-EU.3.7.	INTEGRATED AND ADAPTIVE RESPONSES TO TOXIC EMERGENCIES FOR RAPID TRIAGE: ENGINEERING THE ROADMAP FROM CASUALTY TO PATIENT TO SURVIVOR.	1/09/2015	31/08/2019	12 931 869	11 966 511	H2020-DRS-2014	UK	FI;DE,NL;CZ,EL; NO;ES;UK	CBRN-E		Emergency; Rescue	YES
656198	TRANSIT	H2020-EU.1.3.2.	The daily governance of transit migration in Turkey at European Union borders: The two-way influence of Turkish-European Union border and migration management practices	1/09/2015	31/08/2017	165 599	165 599	H2020-MSCA-IF-2014	NL		Border control		Migration; Social sciences	NO
776355	TransSec	H2020-EU.3.4.2.2.; H2020-EU.3.4.1.2.; H2020-EU.2.1.6.3.; H2020-EU.2.1.6.1.2.	Autonomous emergency manoeuvring and movement monitoring for road transport security	1/02/2018	31/01/2021	3 007 614	2 527 229	H2020-GALILEO-GSA-2017-1	DE	IE;ES;DE;AT	Public spaces; Space	Terrorism & radicalisation	Applications in satellite navigation; Transport	YES
644412	TREDISEC	H2020-EU.2.1.1.	Trust-aware, REliable and Distributed Information SEcurity in the Cloud.	1/04/2015	31/03/2018	6 470 619	4 412 063	H2020-ICT-2014-1	ES	FR;EL;CH; DE;UK;ES	Cybersecurity	Cybercrime	Cloud; ICT	YES
740934	TRIVALENT	H2020-EU.3.7.6.; H2020-EU.3.7.1.	Terrorism pReventlon Via rAdicalisation countEr-NarraTive	1/05/2017	30/04/2020	2 720 420	2 720 420	H2020-SEC-2016-2017-1	IT	IT;PT;PL;BE;ES; FR;LV;AL;IL;UK	Combating radicalisation	Terrorism & radicalisation	Social sciences; Violence	YES
653449	TYPES	H2020-EU.3.7.	Towards transparencY and Privacy in the online advertising businesS	1/05/2015	31/10/2017	4 661 143	3 992 663	H2020-DS-2014-1	ES	EL;ES;BE;IL;UK	Cybersecurity	Cybercrime	Privacy	YES
752743	UCOC	H2020-EU.1.3.2.	Understanding the Commitment in Organized Crime	1/03/2018	28/02/2021	264 668	264 668	H2020-MSCA-IF-2016	FR		Other	Organised crime	Social sciences	NO
653729	Unity	H2020-EU.3.7.	Unity	1/05/2015	30/04/2018	4 538 120	4 330 900	H2020-FCT-2014	UK	BG;DE;BE; ES;MK;UK; HR;EE;NL;FI	Other		Law enforcement	YES
731453	VESEEDIA	H2020-EU.3.7.; H2020-EU.2.1.1.	VERIFICATION ENGINEERING OF SAFETY AND SECURITY CRITICAL DYNAMIC INDUSTRIAL APPLICATIONS	1/01/2017	31/12/2019	4 192 059	4 192 059	H2020-DS-LEIT-2016	AT	FR;ES;DE;FI;HU; BE	Cybersecurity	Cybercrime	IoT	YES
740754	VICTORIA	H2020-EU.3.7.6.; H2020-EU.3.7.1.	Video analysis for Investigation of Criminal and TerrORist Activities	1/05/2017	30/04/2020	5 007 125	5 007 125	H2020-SEC-2016-2017-1	FR	RO;AT;DE; FR;ES;BE;UK	Other	Terrorism & radicalisation; Organised crime	Law enforcement; Surveillance	YES
740580	VISAGE	H2020-EU.3.7.1.; H2020-EU.3.7.7.	Visible Attributes through Genomics: Broadened Forensic Use of DNA for Constructing Composite Sketches from Traces	1/05/2017	30/04/2021	5 007 779	5 000 000	H2020-SEC-2016-2017-1	NL	DE;FR;UK; ES;AT;PL;SE;NL	Other		Forensics	YES
653321	WISER	H2020-EU.3.7.	Wide-Impact cyber SEcurity Risk framework	1/06/2015	30/11/2017	3 396 455	2 562 596	H2020-DS-2014-1	ES	IT;NO;SI;BE;FR; UK	Cybersecurity; Critical infrastructures	Cybercrime		YES
644371	WITDOM	H2020-EU.2.1.1.	empowering prlvcy and securiTy in non-trustedD enviroNments	1/01/2015	31/12/2017	4 020 281	2 764 031	H2020-ICT-2014-1	ES	SI;CH;IT;ES;BE	Cybersecurity	Cybercrime	Privacy; ICT	YES
653866	WOSCAP	H2020-EU.3.7.	Whole-of-Society Conflict Prevention and Peacebuilding	1/06/2015	30/11/2017	2 018 035	1 990 114	H2020-BES-2014	NL	UK;DE;FR; ML;GE;UA;	Defence		Peace keeping; External security	YES

Project id	Project acronym	Programme	Project title	Start Date	End Date	Total Cost (€)	EC Max Contribution (€)	Call	Coordinator Country	Participant Countries	Building block(s)	Priority(ies)	Main focus(es)	Dual Use
										ES;NL;YE				
780498	YAKSHA	H2020-EU.2.1.1.	Cybersecurity Awareness and Knowledge Systemic High-level Application	1/01/2018	30/06/2020	2 506 226	1 998 814	H2020-ICT-2017-1	PT	IT;FI;BG;FR;TH; ES;VN; EL;MY	Cybersecurity	Cybercrime	ICT; Supply chain	YES
725194	CRIMTANG	H2020-EU.1.1.	Criminal Entanglements. A new ethnographic approach to transnational organised crime.	1/02/2018	31/01/2023	1 999 909	1 999 909	ERC-2016-COG	DK		Other	Organised crime	Migration; Social sciences	NO
775989	CBRNE STNDS 2017	H2020-EU.3.7.2.; H2020-EU.3.7.7.; H2020-EU.3.7.5.	ERNICIP CBRNE STANDARDS 2017 and 2018 – support to Mandate 487	1/06/2017	31/05/2019	500 000	500 000	H2020-IBA-SC7-ERNICIP-2017	BE		CBRN-E; Critical infrastructures; Public spaces	Terrorism & radicalisation	Standardisation	YES
753223	NARCOREADER	H2020-EU.1.3.2.	Novel electrochemical strategies for rapid, on-site multiscreening of illicit drugs	1/05/2017	30/04/2019	160 800	160 800	H2020-MSCA-IF-2016	BE		Other	Organised crime	Law enforcement; Forensics	YES
757455	DUST	H2020-EU.1.1.	Data Assimilation for Agent-Based Models: Applications to Civil Emergencies	1/01/2018	31/12/2022	1 499 840	1 499 840	ERC-2017-STG	UK		Other	Terrorism & radicalisation	Emergency; Disaster Management	YES
678341	USECFrontiers	H2020-EU.1.1.	Frontiers of Usable Security – Principles and Methods for Administrator and Developer Usable Security Research	1/08/2016	31/07/2021	1 498 976	1 498 976	ERC-2015-STG	DE		Cybersecurity	Cybercrime		YES
678921	SIREN	H2020-EU.1.1.	Securing Internet Routing from the Ground Up	1/02/2016	31/01/2021	1 468 200	1 468 200	ERC-2015-STG	IL		Cybersecurity	Cybercrime		YES
775707	UNFRAUD	H2020-EU.3.7.; H2020-EU.2.3.1.	An advanced online anti-fraud software equipped with deep learning Artificial Intelligence that can face and detect, current fraudulent techniques and their continued evolution in a cost effective man	1/06/2017	30/09/2017	71 429	50 000	H2020-SMEINST-1-2016-2017	IT		Cybersecurity	Cybercrime		YES
762383	GICA	H2020-EU.3.7.; H2020-EU.2.3.1.	Geolocalisation of Individuals in Critical Areas	1/04/2017	30/09/2017	71 429	50 000	H2020-SMEINST-1-2016-2017	FR		Critical infrastructures	Terrorism & radicalisation	Rescue	YES
733711	FACCESS	H2020-EU.3.7.; H2020-EU.2.3.1.	Enabling the large-scale deployment of Facial Recognition in banking security	1/12/2016	30/11/2018	2 418 000	1 692 600	H2020-SMEINST-2-2016-2017	ES		Cybersecurity	Cybercrime	Biometrics; Privacy	YES
726818	ProBOS	H2020-EU.3.7.; H2020-EU.2.3.1.	Protection Beyond Operating System – Development of the next generation cyber security solution	1/10/2016	30/09/2018	2 814 766	1 970 336	H2020-SMEINST-2-2016-2017	MT		Cybersecurity	Cybercrime		YES
634943	PASS	H2020-EU.2.1.6.	Preparation for the establishment of a European SST Service provision function	1/09/2014	31/12/2016	1 153 250	1 000 000	H2020-Adhoc-2014-20	ES		Space			YES
808316	Radiation detector	H2020-EU.2.1.1.; H2020-EU.2.3.1.	Novel radioactive radiation technology feasibility verification	1/03/2018	30/06/2018	71 429	50 000	H2020-SMEINST-1-2016-2017	FI		Border control; CBRN-E	Organised crime; Terrorism & radicalisation		YES
673980	CyberWiz	H2020-EU.3.7.; H2020-EU.2.3.1.	Cyber-Security Visualization and CAD-Tool for the Vulnerability Assessment of Critical Infrastructures	1/09/2015	31/08/2017	2 279 375	1 595 563	H2020-SMEINST-2-2014	DE	SE	Critical infrastructures; Cybersecurity	Cybercrime		YES

Project id	Project acronym	Programme	Project title	Start Date	End Date	Total Cost (€)	EC Max Contribution (€)	Call	Coordinator Country	Participant Countries	Building block(s)	Priority(ies)	Main focus(es)	Dual Use
685074	IRON	H2020-EU.3.5.; H2020-EU.2.3.1.	High sensitivity multi-gas handheld gas analysis technology	1/09/2015	31/08/2017	3 351 725	2 346 208	H2020-SMEINST-2-2015	FI		CBRN-E			YES
687329	STRIKE3	H2020-EU.2.1.6.	Standardisation of GNSS Threat reporting and Receiver testing through International Knowledge Exchange, Experimentation and Exploitation	1/02/2016	31/01/2019	1 315 429	1 170 615	H2020-Galileo-2015-1	UK	SE;KR;FI;IN;DE; UK	Space; Cybersecurity	Cybercrime	Applications in satellite navigation; Standardisation	YES
690111	SecureCloud	H2020-EU.2.1.1.	Secure Big Data Processing in Untrusted Clouds	1/01/2016	31/12/2018	2 285 377	1 499 627	H2020-EUB-2015	DE	IT;CH;UK;DK;IL	Cybersecurity	Cybercrime	Cloud	YES
703613	DSMM	H2020-EU.1.3.2.	“(De) Securitising Muslims in Cyber space: Social Media, Civil society and Marginalisation After Charlie Hebdo and the Islamic State”	1/10/2016	30/09/2018	173 076	173 076	H2020-MSCA-IF-2015	FR		Combating radicalisation	Terrorism & radicalisation	Social media; Social sciences	YES
783977	Wardiam Perimeter	H2020-EU.3.7.; H2020-EU.2.3.1.	An innovative intruder detection hidden technology based on Controlled Magnetic Fields able to detect threats before happening	1/02/2018	31/07/2019	1 390 600	973 420	H2020-SMEINST-2-2016-2017	ES		Critical infrastructures	Terrorism & radicalisation	Surveillance; Physical threats	YES
784247	IDAaaS	H2020-EU.3.7.; H2020-EU.2.3.1.	Trusted online service for identity assurance	1/10/2017	31/05/2019	1 940 661	1 358 462	H2020-SMEINST-2-2016-2017	NO		Cybersecurity; Terrorism financing	Cybercrime; Organised crime; Terrorism & radicalisation		YES
724725	SWORD	H2020-EU.1.1.	Security Without Obscurity for Reliable Devices	1/09/2017	31/08/2022	1 997 661	1 997 661	ERC-2016-COG	BE		Cybersecurity	Cybercrime	Cryptography	YES
639554	aSCEND	H2020-EU.1.1.	Secure Computation on Encrypted Data	1/06/2015	31/05/2020	1 253 893	1 253 893	ERC-2014-STG	FR		Cybersecurity	Cybercrime	Cryptography; Cloud	YES
694995	BIOSEC	H2020-EU.1.1.	Biodiversity and Security: understanding environmental crime, illegal wildlife trade and threat finance.	1/09/2016	31/08/2020	1 822 729	1 822 729	ERC-2015-AdG	UK		Terrorism financing	Organised crime	Social sciences	NO
704330	ACTING-NOW	H2020-EU.1.3.2.	Algorithmic Containment of Threats in Graphs, Networks or Webs	12/09/2016	11/09/2018	183 455	183 455	H2020-MSCA-IF-2015	UK		Cybersecurity	Cybercrime		YES
639366	FELICITY	H2020-EU.1.1.	Foundations of Efficient Lattice Cryptography	1/10/2015	30/09/2020	1 311 688	1 311 688	ERC-2014-STG	FR		Cybersecurity	Cybercrime	Cryptography	YES
715753	SECOMP	H2020-EU.1.1.	Efficient Formally Secure Compilers to a Tagged Architecture	1/01/2017	31/12/2021	1 498 444	1 498 444	ERC-2016-STG	FR		Cybersecurity	Cybercrime		YES
683032	CIRCUS	H2020-EU.1.1.	An end-to-end verification architecture for building Certified Implementations of Robust, Cryptographically Secure web applications	1/04/2016	31/03/2021	1 885 248	1 885 248	ERC-2015-CoG	FR		Cybersecurity	Cybercrime	Cryptography	YES
659316	CYBERNETS	H2020-EU.1.3.2.	Cybernetic Communication Networks: Fundamental Limits and Engineering Challenges	1/06/2015	31/05/2017	185 076	185 076	H2020-MSCA-IF-2014	FR		Cybersecurity	Cybercrime		YES
746667	AF-Cyber	H2020-EU.1.3.2.	Logic-based Attribution and Forensics in Cyber Security	1/02/2018	31/01/2020	183 455	183 455	H2020-MSCA-IF-2016	UK		Cybersecurity	Cybercrime	Forensics	YES

Project id	Project acronym	Programme	Project title	Start Date	End Date	Total Cost (€)	EC Max Contribution (€)	Call	Coordinator Country	Participant Countries	Building block(s)	Priority(ies)	Main focus(es)	Dual Use
757731	LightCrypt	H2020-EU.1.1.	New Directions in Lightweight Cryptanalysis	1/10/2017	30/09/2022	1 487 500	1 487 500	ERC-2017-STG	IL		Cybersecurity	Cybercrime	Cryptography; IoT	YES
791486	Glyco-DeCon	H2020-EU.3.7.; H2020-EU.2.3.1.	Decontamination by glycosylation based wipes	1/01/2018	30/06/2018	71 429	50 000	H2020-SMEINST-1-2016-2017	IE		CBRN-E	Terrorism & radicalisation		YES
790554	Genomcore Identity	H2020-EU.3.7.; H2020-EU.2.3.1.	Genomcore Identity: databank proxy for DNA fingerprinting from whole exome/genome for biometric identification	1/01/2018	30/06/2018	71 429	50 000	H2020-SMEINST-1-2016-2017	ES		Other		Biometrics; Law enforcement; Forensics	YES
791727	ProtonSuite	H2020-EU.3.7.; H2020-EU.2.3.1.	The world's largest secure collaboration suite	1/12/2017	31/03/2018	71 429	50 000	H2020-SMEINST-1-2016-2017	CH		Cybersecurity	Cybercrime	Privacy	YES
791208	V-SPHERE	H2020-EU.3.7.; H2020-EU.2.3.1.	Vulnerability Search and Prevention through Holistic End-to-end Risk Evaluation	1/02/2018	31/05/2018	71 429	50 000	H2020-SMEINST-1-2016-2017	NO		Cybersecurity	Cybercrime		YES
790798	PMT4NIIS	H2020-EU.3.7.; H2020-EU.2.3.1.	Predictive Maintenance Tool for Non-Intrusive Inspection Systems	1/01/2018	30/06/2018	71 429	50 000	H2020-SMEINST-1-2016-2017	BG		Border control	Organised crime; Terrorism & radicalisation	Supply chain	YES
778571	Smart-Trust	H2020-EU.3.7.; H2020-EU.2.3.1.	Smart Trust: Secure Mobile ID for Trusted Smart Borders	1/01/2018	31/12/2019	2 991 000	2 093 700	H2020-SMEINST-2-2016-2017	PT		Border control	Terrorism & radicalisation	Biometrics; Blockchain	YES
651669	CAPTOR	H2020-EU.3.7.; H2020-EU.2.3.1.	cAPTOr captures Advanced System Threats	1/10/2014	28/02/2015	71 429	50 000	H2020-SMEINST-1-2014	ES		Critical infrastructures; Public spaces; Cybersecurity	Terrorism & radicalisation; Cybercrime		YES
740146	NESPINT	H2020-EU.3.7.; H2020-EU.2.3.1.	NEutron Spectrometry to Prevent Illicit Nuclear Trafficking	1/01/2017	30/06/2017	71 429	50 000	H2020-SMEINST-1-2016-2017	IT		Border control; CBRN-E	Organised crime		YES
781524	UR Browser	H2020-EU.2.1.1.; H2020-EU.2.3.1.	The first all-European web browser capable of guaranteeing comprehensive online privacy and security for EU Internet users	1/06/2017	30/09/2017	71 429	50 000	H2020-SMEINST-1-2016-2017	FR		Cybersecurity	Cybercrime	Privacy	YES
745088	NK-52-2016	H2020-EU.3.7.; H2020-EU.2.3.1.	Next generation authentication for the digital age	1/04/2017	30/09/2017	71 429	50 000	H2020-SMEINST-1-2016-2017	LV		Cybersecurity	Cybercrime		YES
712120	TRUEPIVOT	H2020-EU.3.7.; H2020-EU.2.3.1.	Advanced engineering analytics for the detection of errors in the structural design of critical urban infrastructure.	1/02/2016	31/07/2016	71 429	50 000	H2020-SMEINST-1-2015	IE		Critical infrastructures	Terrorism & radicalisation	Physical threats	YES
673627	SafeSky	H2020-EU.3.7.; H2020-EU.2.3.1.	SafeSky - Integrated system for critical infrastructure and personal sphere monitoring and protection against aerial threats	1/07/2015	31/10/2015	71 429	50 000	H2020-SMEINST-1-2014	PL	PL	Critical infrastructures; Public spaces	Terrorism & radicalisation		YES
674422	PreserviX	H2020-EU.2.1.1.; H2020-EU.2.3.1.	Reshaping Digital Preservation	1/05/2015	31/10/2015	71 429	50 000	H2020-SMEINST-1-2014	NO		Cybersecurity	Cybercrime	ICT	YES
674563	ART	H2020-EU.3.7.; H2020-EU.2.3.1.	Feasibility assessment on Alarm Resolution Technology, using X-Ray Echo Methodology	1/06/2015	31/10/2015	71 429	50 000	H2020-SMEINST-1-2014	NL		Border control; CBRN-E	Terrorism & radicalisation; Organised crime		YES

Project id	Project acronym	Programme	Project title	Start Date	End Date	Total Cost (€)	EC Max Contribution (€)	Call	Coordinator Country	Participant Countries	Building block(s)	Priority(ies)	Main focus(es)	Dual Use
663680	Starlight	H2020-EU.3.7.; H2020-EU.2.3.1.	Demonstration of a High Definition Low Light Sensor (Starlight) for use in the Surveillance and Protection of Urban Soft Targets and Critical Infrastructures.	1/06/2015	30/11/2015	71 429	50 000	H2020-SMEINST-1-2014	UK		Critical infrastructures; Public spaces	Terrorism & radicalisation	Surveillance	YES
707135	GenoPri	H2020-EU.1.3.2.	Quantifying and Protecting the Privacy of Genomic Data	1/05/2016	30/04/2018	157 846	157 846	H2020-MSCA-IF-2015	TR		Cybersecurity	Cybercrime	Privacy	YES
679924	QINTERNET	H2020-EU.1.1.	Quantum communication networks	1/03/2016	28/02/2021	1 498 725	1 498 725	ERC-2015-STG	NL		Cybersecurity	Cybercrime	Cryptography	YES
648608	EXCHANGE	H2020-EU.1.1.	Forensic Geneticists and the Transnational Exchange of DNA data in the EU: Engaging Science with Social Control, Citizenship and Democracy	1/10/2015	30/09/2020	1 838 150	1 838 150	ERC-2014-CoG	PT		Other	Organised crime; Terrorism & radicalisation	Ethical dimension	NO
672045	Smart firearm safety	H2020-EU.2.1.1.; H2020-EU.2.3.1.	Project iP9 Smart firearm safety Introduction of the first smart firearm safety to the institutional market (police)	1/04/2015	30/09/2015	71 429	50 000	H2020-SMEINST-1-2014	DE		Other		Law enforcement; Certification; ICT	YES
662784	Gait Biometrics 3	H2020-EU.2.1.1.; H2020-EU.2.3.1.	Main goal of the project is to create a prototype of the software, which will be able to identify people just based on the way how they walk.	1/02/2015	31/07/2015	71 429	50 000	H2020-SMEINST-1-2014	CZ		Public spaces	Terrorism & radicalisation	Biometrics; Law enforcement; ICT; Forensics	YES
684761	SPIN	H2020-EU.2.1.1.; H2020-EU.2.3.1.	Secure and protected interoperability	1/07/2015	31/12/2015	71 429	50 000	H2020-SMEINST-1-2015	SE		Cybersecurity	Cybercrime	Information exchange; ICT	YES
650796	SignSigma	H2020-EU.2.1.1.; H2020-EU.2.3.1.	Launching the next generation of mobile and multi-platform signature system based on biometric parameters	1/09/2014	30/11/2014	71 429	50 000	H2020-SMEINST-1-2014	ES		Cybersecurity	Cybercrime	Biometrics; ICT	YES
684168	Excalibur 2.0	H2020-EU.2.1.1.; H2020-EU.2.3.1.	Revolutionary trustworthy platform for seamless authentication of Internet users	1/06/2015	31/08/2015	71 429	50 000	H2020-SMEINST-1-2015	PL		Cybersecurity	Cybercrime	Cryptography; ICT	YES
684458	REVEN-X1	H2020-EU.2.1.1.; H2020-EU.2.3.1.	REVEN-X1: Automatic Vulnerability Detection in Binary	1/07/2015	31/12/2015	71 429	50 000	H2020-SMEINST-1-2015	FR		Cybersecurity; Critical infrastructures	Cybercrime	ICT	YES
696828	NED- Nano Eye Device	H2020-EU.2.3.1.; H2020-EU.2.1.2.	THE NANO EYE DEVICE	1/09/2015	31/01/2016	71 429	50 000	H2020-SMEINST-1-2015	IT		Other	Terrorism & radicalisation		YES
674379	ACT4INFRA	H2020-EU.3.7.; H2020-EU.2.3.1.	Innovative Actuators for empowering smart pipeline infrastructures towards secure water, gas and heating supply	1/07/2015	31/12/2015	71 429	50 000	H2020-SMEINST-1-2014	DE		Critical infrastructures	Terrorism & radicalisation		YES
663815	LineVu	H2020-EU.3.7.; H2020-EU.2.3.1.	A novel optical sensor platform for detection and measurement of contaminants in gas pipelines to protect critical infrastructure from disruption and damage - Linevu	1/03/2015	31/08/2015	71 429	50 000	H2020-SMEINST-1-2014	UK		Critical infrastructures	Terrorism & radicalisation	Supply security; Surveillance	YES
662822	Invest	H2020-EU.3.7.; H2020-EU.2.3.1.	INtelligent Video analytics to analyse complex scenes and Enhance Security of critical infrastructure and urban soft Targets	1/01/2015	30/06/2015	71 429	50 000	H2020-SMEINST-1-2014	UK		Critical infrastructures; Public spaces	Terrorism & radicalisation	Law enforcement; Surveillance	YES
664032	BIWAS	H2020-EU.3.7.; H2020-EU.2.3.1.	Biological Water Alarm System (BiWAS) for protection of urban drinking water infrastructure against CBRN threats	1/02/2015	31/07/2015	71 429	50 000	H2020-SMEINST-1-2014	NO	SE	Critical infrastructures; CBRN-E	Terrorism & radicalisation		YES

Project id	Project acronym	Programme	Project title	Start Date	End Date	Total Cost (€)	EC Max Contribution (€)	Call	Coordinator Country	Participant Countries	Building block(s)	Priority(ies)	Main focus(es)	Dual Use
719660	OneCard	H2020-EU.3.7.; H2020-EU.2.3.1.	Increasing the security of access to urban critical infrastructure with a Near Field Communication micro SD smart card for mobile devices using on-chip state of the art technology	1/03/2016	31/05/2016	71 429	50 000	H2020-SMEINST-1-2015	SK		Critical infrastructures	Terrorism & radicalisation		YES
684849	Loca Credibilia	H2020-EU.3.7.; H2020-EU.2.3.1.	Data and document integrity for services provided through critical information infrastructures	1/05/2015	31/10/2015	71 429	50 000	H2020-SMEINST-1-2015	HU		Cybersecurity; Critical infrastructures	Cybercrime		YES
712317	QuardCard	H2020-EU.3.7.; H2020-EU.2.3.1.	Powered smart card with a biometric one time password system	1/04/2016	31/08/2016	71 429	50 000	H2020-SMEINST-1-2015	DK	DK	Cybersecurity	Cybercrime	Biometrics	YES
719382	DAPS	H2020-EU.3.7.; H2020-EU.2.3.1.	Drone Alarm and Protection System	1/01/2016	31/05/2016	71 429	50 000	H2020-SMEINST-1-2015	DK		Critical infrastructures; Public spaces	Terrorism & radicalisation	UAV	YES
710770	PROTECT-2	H2020-EU.3.7.; H2020-EU.2.3.1.	PeRsonnel lOcation and Tracking for safEty of Critical InfrasTructures	1/03/2016	31/08/2016	71 429	50 000	H2020-SMEINST-1-2015	IT		Critical infrastructures; Public spaces	Terrorism & radicalisation		YES
672428	UPAC S-100	H2020-EU.3.7.; H2020-EU.2.3.1.	Feasibility study for URBAN PROTECTION AVIATION COPTER S-100	1/07/2015	31/12/2015	71 429	50 000	H2020-SMEINST-1-2014	AT		Critical infrastructures; Public spaces; Border control	Terrorism & radicalisation	UAV; Surveillance; Disaster management	YES
717736	WARDIAM PERIMETER	H2020-EU.3.7.; H2020-EU.2.3.1.	WARDIAM PERIMETER	1/04/2016	30/09/2016	71 429	50 000	H2020-SMEINST-1-2015	ES		Critical infrastructures; Public spaces	Terrorism & radicalisation	Surveillance	YES
650476	SmartPatch	H2020-EU.3.7.; H2020-EU.2.3.1.	Use of a cost effective smart skin sensor system for remote Structural Health Monitoring and post event structural damage assessment in Soft Urban Targets and Critical Infrastructures Protection	1/07/2014	31/12/2014	71 429	50 000	H2020-SMEINST-1-2014	IT		Critical infrastructures; Public spaces	Terrorism & radicalisation	Emergency; Disaster management	YES
673969	Bio-AX	H2020-EU.3.7.; H2020-EU.2.3.1.	A new wearable, cost effective and non-invasive biometric solution for accurate and high throughput screening of people, bags and vehicles	1/06/2015	31/08/2015	71 429	50 000	H2020-SMEINST-1-2014	UK		Border control; Public spaces	Terrorism & radicalisation	Biometrics	YES
684441	AIRS	H2020-EU.3.7.; H2020-EU.2.3.1.	Advanced Intelligent Raman System for detection of explosives and harmful substances at urban soft targets	1/09/2015	29/02/2016	71 429	50 000	H2020-SMEINST-1-2015	UK		Public spaces; CBRN-E; Border control	Terrorism & radicalisation		YES
697593	OMIS	H2020-EU.3.7.; H2020-EU.2.3.1.	Optical Mid Infrared Spectrometer	1/11/2015	30/04/2016	71 429	50 000	H2020-SMEINST-1-2015	IT		Critical infrastructures	Terrorism & radicalisation		YES
696917	FACCESS	H2020-EU.3.7.; H2020-EU.2.3.1.	Enabling the large-scale deployment of Facial Recognition in banking security	1/09/2015	31/01/2016	71 429	50 000	H2020-SMEINST-1-2015	ES		Cybersecurity	Cybercrime	Biometrics; Ethical dimension	YES
684759	INNOPROCITI	H2020-EU.3.7.; H2020-EU.2.3.1.	INNOVATIVE ENZYMES TO PROTECT CITIZENS AND CRITICAL INFRASTRUCTURES	1/09/2015	29/02/2016	71 429	50 000	H2020-SMEINST-1-2015	IT		Critical infrastructures; Border control; CBRN-E	Terrorism & radicalisation		YES
674434	SMS	H2020-EU.3.7.; H2020-EU.2.3.1.	SMS - Safety Micro Sensor	1/07/2015	31/12/2015	71 429	50 000	H2020-SMEINST-1-2014	IT	IT	CBRN-E; Critical infrastructures; Public spaces	Terrorism & radicalisation		YES

Project id	Project acronym	Programme	Project title	Start Date	End Date	Total Cost (€)	EC Max Contribution (€)	Call	Coordinator Country	Participant Countries	Building block(s)	Priority(ies)	Main focus(es)	Dual Use
650513	SURVEIRON	H2020-EU.3.7.; H2020-EU.2.3.1.	SURVEIRON: Advanced surveillance system for the protection of urban soft targets and urban critical infrastructures	1/09/2014	28/02/2015	71 429	50 000	H2020-SMEINST-1-2014	ES		Critical infrastructures; Public spaces	Terrorism & radicalisation	UAV; Surveillance; Emergency	YES
673138	SENEX	H2020-EU.3.7.; H2020-EU.2.3.1.	Table Top Device based on Nanostructured Sensors for the continuous ENvironmental monitoring of EXplosive substances in sensitive areas	1/07/2015	31/12/2015	71 429	50 000	H2020-SMEINST-1-2014	IT		Border control; Critical infrastructures; CBRN-E	Terrorism & radicalisation		YES
651272	HOLOSCAN	H2020-EU.3.7.; H2020-EU.2.3.1.	Holographic Scanner for Safe Real-Time High Throughput Screening of People and Their Bags	1/12/2014	31/05/2015	71 429	50 000	H2020-SMEINST-1-2014	NO		Public spaces; Border control	Terrorism & radicalisation		YES
735092	SK PRES SSH	H2020-EU.3.6.	Social Sciences and Humanities: a New Agenda for Europe's Challenges	1/09/2016	31/08/2017	150 000	150 000	H2020-Adhoc-2014-20	SK		Combating radicalisation	Terrorism & radicalisation	Social sciences	NO
700176	SISSDEN	H2020-EU.3.7.	Secure Information Sharing Sensor Delivery event Network	1/05/2016	30/04/2019	6 341 775	4 912 693	H2020-DS-2015-1	PL	UK;CH;NL; FR;IT;DE	Cybersecurity	Cybercrime	Law enforcement	YES
711264	SURVEIRON	H2020-EU.3.7.; H2020-EU.2.3.1.	SURVEIRON: Advanced surveillance system for the protection of urban soft targets and urban critical infrastructures	1/03/2016	28/02/2018	2 479 593	1 735 715	H2020-SMEINST-2-2015	ES		Critical infrastructures; Public spaces	Terrorism & radicalisation	UAV; Surveillance; Emergency; Disaster management	YES
696945	IMPRINT	H2020-EU.3.7.; H2020-EU.2.3.1.	Defeat of Insider Theft in Nuclear and Radioactive Sites	1/12/2015	30/11/2017	1 474 325	1 032 027	H2020-SMEINST-2-2015	IL		CBRN-E	Terrorism & radicalisation		YES
719806	BIO-AX	H2020-EU.3.7.; H2020-EU.2.3.1.	A novel wearable, cost-effective and non-invasive biometric body worn video solution for accurate and high throughput screening of people, bags and vehicles	1/03/2016	28/02/2018	1 103 261	772 283	H2020-SMEINST-2-2015	UK		Public spaces; Border control	Terrorism & radicalisation	Biometrics	YES
674274	SPIDERS	H2020-EU.3.7.; H2020-EU.2.3.1.	Synthetic aPerture Interferometric raDiometer for sEcurity in cRitical infraStructures	1/10/2015	31/05/2018	1 166 000	816 200	H2020-SMEINST-2-2014	FR		Critical infrastructures; Public spaces; Border control	Terrorism & radicalisation		YES
696973	HDIV	H2020-EU.3.7.; H2020-EU.2.3.1.	HDIV: SELF-PROTECTED WEB APPLICATIONS	1/11/2015	31/10/2017	1 325 000	927 500	H2020-SMEINST-2-2015	ES		Critical infrastructures; Cybersecurity	Cybercrime		YES
666490	AquaSHIELD	H2020-EU.3.7.; H2020-EU.2.3.1.	Protecting citizens against intentional drinking water contamination with a water quality firewall	1/01/2015	31/05/2017	1 123 136	786 195	H2020-SMEINST-2-2014	NL		Critical infrastructures; Public spaces	Terrorism & radicalisation	Physical threats	YES
672001	ACES	H2020-EU.3.7.; H2020-EU.2.3.1.	ACES: Air Cargo Explosive Screener	1/10/2015	30/09/2017	1 233 329	863 330	H2020-SMEINST-2-2014	ES		Critical infrastructures; CBRN-E; Public spaces	Terrorism & radicalisation	Certification; Transport	YES
666432	CITRIMACC	H2020-EU.3.4.; H2020-EU.2.3.1.	Circulation Pilot with Continuous Control of Multi-Modal Air Cargo Containers	1/08/2015	31/07/2017	3 412 665	2 388 865	H2020-SMEINST-2-2014	NL	UK;NL;LU	Border control; Critical infrastructures	Terrorism & radicalisation	Transport	YES
640652	DCM	H2020-EU.1.1.	Distributed Cryptography Module	1/11/2014	30/04/2016	149 776	149 776	ERC-2014-PoC	IL		Cybersecurity	Cybercrime	Cryptography	YES

Project id	Project acronym	Programme	Project title	Start Date	End Date	Total Cost (€)	EC Max Contribution (€)	Call	Coordinator Country	Participant Countries	Building block(s)	Priority(ies)	Main focus(es)	Dual Use
673336	CLAPPRO	H2020-EU.2.1.1.; H2020-EU.2.3.1.	Cloud Protection: Centralized encryption technology for file sharing	1/07/2015	30/06/2017	871 615	610 131	H2020-SMEINST-2-2014	ES		Cybersecurity	Cybercrime	Cryptography; Cloud; ICT	YES
719375	QR-PATROL PRO	H2020-EU.2.1.1.; H2020-EU.2.3.1.	A cost effective cloud-based platform for delivering the highest level of security, supervision and management for security companies utilizing Push-to-Talk and Internet of Things technologies.	1/07/2016	30/06/2018	1 927 423	1 349 196	H2020-SMEINST-2-2015	EL		Other	Cybercrime	IoT	YES
697515	KMaaS	H2020-EU.2.1.1.; H2020-EU.2.3.1.	Key Management as-a-Service	1/02/2016	31/01/2018	3 259 375	2 281 563	H2020-SMEINST-2-2015	DK	DK	Cybersecurity	Cybercrime	Cryptography; Cloud; ICT	YES
666287	PAYPLUG LABS	H2020-EU.2.1.1.; H2020-EU.2.3.1.	Next generation online payments and fraud detection API for European SMEs	1/06/2015	31/12/2017	2 977 725	1 750 000	H2020-SMEINST-2-2014	FR		Cybersecurity	cybercrime	ICT	YES
767542	INSIKT	H2020-EU.3.7.; H2020-EU.2.3.1.	Novel Social Data Mining Platform to Detect and Defeat Violent Online Radicalization	1/10/2017	30/09/2019	2 190 219	1 533 153	H2020-SMEINST-2-2016-2017	ES		Combating radicalisation	Terrorism & radicalisation	Law enforcement; Social media	YES
772665	3ants	H2020-EU.3.7.; H2020-EU.2.3.1.	Enhancing security of digital property rights and citizens' awareness through an innovative anti-piracy framework of digital content based on Machine Learning and Artificial Intelligence	1/07/2017	31/12/2017	71 429	50 000	H2020-SMEINST-1-2016-2017	ES		Cybersecurity	Cybercrime		YES
747249	PyroProf	H2020-EU.1.3.2.	Chemical Profiling of Inorganic and Pyrotechnic Explosives	4/09/2017	3/09/2019	177 599	177 599	H2020-MSCA-IF-2016	NL		CBRN-E	Terrorism & radicalisation	Forensics; Law enforcement	YES
750348	CPR	H2020-EU.1.3.2.	A cross-country comparison of Communications designed to Prevent Radicalisation	1/11/2017	31/10/2019	200 195	200 195	H2020-MSCA-IF-2016	DK		Combating radicalisation	Terrorism & radicalisation	Social sciences	YES
736783	Zoovel-UC	H2020-EU.3.7.; H2020-EU.2.3.1.	Inaudible SMART CROWDS SECURITY through existing loudspeakers"	1/10/2016	31/03/2017	71 429	50 000	H2020-SMEINST-1-2016-2017	ES		Public spaces	Terrorism & radicalisation	Violence	YES
739685	SecIoT	H2020-EU.2.3.2.2.	Cybersecurity Threat Detection for Internet of Things Connected Devices	1/09/2017	31/08/2018	117 844	117 844	H2020-INNOSUP-02-2016	UK		Cybersecurity	cybercrime	IoT	YES
745114	X5 bitworker	H2020-EU.2.1.1.; H2020-EU.2.3.1.	X5 bitworker - The Copying System for the Internet of Things and Industry 4.0	1/12/2016	31/05/2017	71 429	50 000	H2020-SMEINST-1-2016-2017	AT		Cybersecurity	cybercrime	IoT	YES
749314	RefBORDER	H2020-EU.1.3.2.	Reflexivity as capacity in EU's border security: a contribution to theory and practice through the case of Polish Border Guard training	1/09/2017	31/08/2019	183 455	183 455	H2020-MSCA-IF-2016	UK		Border control	Terrorism & radicalisation	Ethical dimension	NO
744484	INSTET	H2020-EU.3.7.; H2020-EU.2.3.1.	Integral Security Trust Element for the Internet of Things	1/10/2016	31/03/2017	71 429	50 000	H2020-SMEINST-1-2016-2017	NL		Cybersecurity	cybercrime	IoT	YES
774256	ePatriot	H2020-EU.3.7.; H2020-EU.2.3.1.	Evolved Sky Patriot – Phase 1 Feasibility Study	1/07/2017	31/12/2017	71 429	50 000	H2020-SMEINST-1-2016-2017	UK		Critical infrastructures	Terrorism & radicalisation	Law enforcement; UAV	YES
672109	Andrupos	H2020-EU.3.; H2020-EU.2.	Automatic non-destructive recognition of used printing techniques on substrates	1/07/2017	31/12/2019	1 753 434	1 269 421	H2020-FTIPilot-2016-1	DE	DE;NL;UK	Border control	Organised crime; Terrorism & radicalisation	Law enforcement; Forensics	YES

Project id	Project acronym	Programme	Project title	Start Date	End Date	Total Cost (€)	EC Max Contribution (€)	Call	Coordinator Country	Participant Countries	Building block(s)	Priority(ies)	Main focus(es)	Dual Use
739799	IPISA	H2020-EU.2.3.2.2.	Inkjet Printed Sensor Arrays for high efficient, low cost, environmental monitoring	1/09/2017	31/08/2018	108 750	108 750	H2020-INNOSUP-02-2016	CY		Public spaces	Terrorism & radicalisation		YES
726317	IPCOM	H2020-EU.3.7.; H2020-EU.2.3.1.	Next generation IP-based smart Push-to-Talk communication device for public security	1/07/2016	30/06/2018	2 446 250	1 712 375	H2020-SMEINST-2-2016-2017	FI		Other		Law enforcement; Communication technologies	YES
781271	UltraFiBi	H2020-EU.3.7.; H2020-EU.2.3.1.	Next-generation Strong Ultrasonic Fingerprint Biometrics	1/10/2017	31/03/2018	71 429	50 000	H2020-SMEINST-1-2016-2017	FR		Other		Biometrics	YES
781027	ARIA	H2020-EU.3.7.; H2020-EU.2.3.1.	Advanced ultra-wideband Radar for Integrated Applications	1/08/2017	30/11/2017	71 429	50 000	H2020-SMEINST-1-2016-2017	IT		Other		Surveillance	YES
763240	CHINO	H2020-EU.3.7.; H2020-EU.2.3.1.	The Health Data Security Platform for EU Developers Enterprises	1/01/2017	30/06/2017	71 429	50 000	H2020-SMEINST-1-2016-2017	IT		Cybersecurity	cybercrime	Privacy	YES
768242	KNOX	H2020-EU.3.7.; H2020-EU.2.3.1.	Cost advantageous and scalable drone alarm and protection system for urban contexts	1/08/2017	31/07/2019	1 804 500	1 258 775	H2020-SMEINST-2-2016-2017	DK		Public spaces; Critical infrastructures	Terrorism & radicalisation	UAV	YES
767383	COUNTERCRAFT	H2020-EU.3.7.; H2020-EU.2.3.1.	Intelligence campaigns in the digital realms	1/09/2017	31/08/2019	1 619 375	1 133 563	H2020-SMEINST-2-2016-2017	ES		Cybersecurity	Cybercrime		YES
775593	GO 4G	H2020-EU.3.7.; H2020-EU.2.3.1.	InvizBox Go 4G - Security and Privacy, Everywhere	1/07/2017	31/12/2017	71 429	50 000	H2020-SMEINST-1-2016-2017	IE		Cybersecurity	Cybercrime	Privacy	YES
775636	MASS	H2020-EU.3.4.; H2020-EU.2.1.1.; H2020-EU.2.3.1.	Micro AIS Shore Station - MASS	1/06/2017	30/11/2017	71 429	50 000	H2020-SMEINST-1-2016-2017	TR		Border control	Organised crime	Surveillance	YES
757096	QuardCard	H2020-EU.3.7.; H2020-EU.2.3.1.	Powered smart card with a biometric one time password system	1/02/2017	31/01/2019	2 314 632	1 620 243	H2020-SMEINST-2-2016-2017	DK	DK	Cybersecurity	Cybercrime	Biometrics	YES
739367	ColdNano-X	H2020-EU.3.7.; H2020-EU.2.3.1.	ZnO-nanotech cold cathode x-ray tube for the security market	1/10/2016	31/12/2018	2 730 653	1 911 457	H2020-SMEINST-2-2016-2017	SE		Border control; Public spaces	Terrorism & radicalisation		YES
743996	U2PIA	H2020-EU.3.7.; H2020-EU.2.3.1.	Universal application 2 conduct Privacy Impact Assessment analysis and reports	1/11/2016	31/03/2017	71 429	50 000	H2020-SMEINST-1-2016-2017	IT		Cybersecurity	Cybercrime	Privacy	YES
744926	I-MUST	H2020-EU.3.7.; H2020-EU.2.3.1.	A handheld, ultra-sensitive device for rapid contactless explosive vapour detection in open air, based on Ion Mobility Universal Sensor Technology	1/12/2016	31/03/2017	71 429	50 000	H2020-SMEINST-1-2016-2017	NL		Public spaces; Border control; CBRN-E	Terrorism & radicalisation		YES
744397	PerfectDashboard 2.0	H2020-EU.3.7.; H2020-EU.2.3.1.	First single platform for efficient and security aware management of CMS based websites	1/10/2016	31/12/2016	71 429	50 000	H2020-SMEINST-1-2016-2017	PL		Cybersecurity	Cybercrime		YES
743831	DNA TRUSTAG	H2020-EU.3.7.; H2020-EU.2.3.1.	DNA TRUSTAG - A paradigm shift in authentication technologies	1/01/2017	31/05/2017	71 429	50 000	H2020-SMEINST-1-2016-2017	PT		Other	Organised crime	Forensics	YES

Project id	Project acronym	Programme	Project title	Start Date	End Date	Total Cost (€)	EC Max Contribution (€)	Call	Coordinator Country	Participant Countries	Building block(s)	Priority(ies)	Main focus(es)	Dual Use
736300	Eye-O-T	H2020-EU.3.7.; H2020-EU.2.3.1.	Cyber security system with a high IoT network visibility and fast vulnerability detection for Smart Homes.	1/08/2016	31/12/2016	71 429	50 000	H2020-SMEINST-1-2016-2017	IL		Cybersecurity	Cybercrime	IoT	YES
735630	SCR	H2020-EU.3.7.; H2020-EU.2.3.1.	Disruptive Cybersecurity SaaS for SMEs and freelance developers	1/07/2016	31/12/2016	71 429	50 000	H2020-SMEINST-1-2016-2017	UK		Cybersecurity	cybercrime	IoT	YES
735734	ThreatMark	H2020-EU.3.7.; H2020-EU.2.3.1.	Advanced Fraud Detection System - Protecting digital transactions against cyber attacks	1/08/2016	30/11/2016	71 429	50 000	H2020-SMEINST-1-2016-2017	CZ		Cybersecurity	Cybercrime		YES
735472	NASUM	H2020-EU.3.7.; H2020-EU.2.3.1.	Innovative nanotech-based detection equipment in the area of homeland security	1/10/2016	31/01/2017	71 429	50 000	H2020-SMEINST-1-2016-2017	IT		Critical infrastructures; Public spaces	Terrorism & radicalisation; Organised crime		YES
729165	BISS	H2020-EU.2.1.1.; H2020-EU.2.3.1.	Biometric Identification Security System	1/06/2016	30/11/2016	71 429	50 000	H2020-SMEINST-1-2016-2017	AT		Cybersecurity	Cybercrime	Biometrics	YES
728408	iNTACT	H2020-EU.3.7.; H2020-EU.2.3.1.	Commercialisation of the world's first iNTelligent Access Cover Technology for the protection of ALL underground infrastructure.	1/05/2016	31/07/2016	71 429	50 000	H2020-SMEINST-1-2016-2017	UK		Critical infrastructures	Terrorism & radicalisation		YES
728532	IDENTITY	H2020-EU.3.7.; H2020-EU.2.3.1.	Usable Digital Signature	1/07/2016	31/12/2016	71 429	50 000	H2020-SMEINST-1-2016-2017	ES		Cybersecurity	cybercrime	Cloud	YES
728516	ConnectProtect	H2020-EU.3.7.; H2020-EU.2.3.1.	A total cyber protection service to Small Businesses operating critical infrastructure and Residential customers	1/07/2016	31/12/2016	71 429	50 000	H2020-SMEINST-1-2016-2017	UK		Cybersecurity	Cybercrime		YES
728673	StandBy-U	H2020-EU.3.7.; H2020-EU.2.3.1.	Real Time Response System towards Safety and Emergency Management Improvement in critical infrastructures and soft targets	1/06/2016	31/08/2016	71 429	50 000	H2020-SMEINST-1-2016-2017	NL		Critical infrastructures; Public spaces	Terrorism & radicalisation	Emergency	YES
728649	LipVerify	H2020-EU.3.7.; H2020-EU.2.3.1.	Feasibility study on the development of LipVerify - a new viseme based user authentication service.	1/07/2016	31/12/2016	71 429	50 000	H2020-SMEINST-1-2016-2017	UK		Cybersecurity	Cybercrime	Biometrics	YES
740189	EuroBioTox	H2020-EU.3.7.1.; H2020-EU.3.7.5.	European programme for the establishment of validated procedures for the detection and identification of biological toxins	1/06/2017	31/05/2022	9 526 721	7 998 747	H2020-SEC-2016-2017-1	DE	SE;FI;BE;FR;UK; CH;DE	CBRN-E	Terrorism & radicalisation		YES
713762	3SST2015	H2020-EU.2.1.6.	Third funding line in 2015 for the establishment of a European SST service provision function	1/01/2016	31/12/2017	9 017 433	9 000 000	H2020-Adhoc-2014-20	IT	ES;DE;UK;FR	Space		Surveillance	YES
763702	PercEvite	H2020-EU.3.4.7.	PercEvite - Sense and avoid technology for small drones	1/09/2017	31/08/2020	899 008	899 008	H2020-SESAR-2016-1	NL	NL;FR;BE	Other		UAV	YES

Annex 5. Data from the analysis of Horizon 2020 security- and defence-related projects

Table 11: Distribution of projects by building block

Building block	Number of projects	Share of projects
Cybersecurity	167	48%
Critical infrastructures	68	19%
Public spaces	43	12%
Border control	39	11%
CBRN-E	24	7%
Radicalisation	18	5%
Space	10	3%
Defence*	9	3%
Terrorism financing*	7	2%
Hybrid threats*	3	1%
Critical supplies*	2	1%
Other (outside building blocks)	48	14%
Total	349	

Note: *Building blocks with fewer than 10 projects.

Source: JRC analysis of Cordis data.

Table 12: Distribution of projects by number of building blocks to which they contribute

Number of building blocks	Number of projects	Share of projects
1 building block	274	79%
2 building blocks	61	17%
3 building blocks	14	4%
Total	349	

Source: JRC analysis of Cordis data.

Table 13: Number of projects related to different building block

	Cyber-security	Critical infrastructures	Public spaces	Border control	CBRN-E	Combating radicalisation	Space	Defence	Terrorism financing	Hybrid threats	Critical supplies	No other building block
Cybersecurity		21	3	1		2	3		3	2		134
Critical infrastructures	21		26	7	7					1		18
Public spaces	3	26		9	6		2					9
Border control	1	7	9		8		1					20
CBRN-E		7	6	8								9
Combating radicalisation	2								1			15
Space	3		2	1								4
Defence*												9
Terrorism financing*	3					1						3
Hybrid threats*	2	1										1
Critical supplies*												2

Note: *Building blocks with fewer than 10 projects.

Source: JRC analysis of Cordis data.

Table 14: Distribution of projects by priority

Priority	Number of projects	Share of projects
Cybercrime	169	48%
Terrorism and radicalisation	120	34%
Organised crime	46	13%
Outside priorities	49	14%
Total	349	

Source: JRC analysis of Cordis data.

Table 15: Distribution of projects by number of priorities to which they contribute

Number of priorities	Number of projects	Share in total projects belonging to priorities
1 priority	266	89%
2 priorities	33	11%
3 priorities	1	0.3%

Source: JRC analysis of Cordis data.

Table 16: Distribution of projects by priority and building block

	Priority			
	Cybercrime	Terrorism and radicalisation	Organised crime	Outside priority
Building block	Number of projects			
Border control	1	25	17	6
Critical infrastructures	21	52	3	
Public spaces	3	40	3	1
Critical supplies				2
Cybersecurity	167	9	4	
CBRN-E		19	4	3
Hybrid threats	2	2		1
Radicalisation	2	18	1	
Terrorism financing	3	4	5	
Space	3	2	1	4
Defence		1	1	8
Other (outside building blocks)	2	10	17	25

Source: JRC analysis of Cordis data.

Table 17: Number of projects by main focus

Main focus	Number of projects
ICT	41
Law enforcement	40
Social sciences	34
Cryptography	31
Privacy	27
IoT	25
Cloud	22
Surveillance	22
Biometrics	22
Forensics	17
UAV	15
Emergency	12
Social media	12
External security	11
Violence	10
Transport	9
Disaster management	9
Physical threats	9
Migration	9
Applications in satellite navigation	8
Ethical dimension	8
Resilience	8
CPS	7
Rescue	6
Peace keeping	6
Supply chain	5
Training	5
Blockchain	5
Certification	4
Preparedness	4
Standardisation	4
Supply security	3
Information exchange	3

Source: JRC analysis of Cordis data.

Table 18: Number of projects by building block and main focus

Building block / Main focus	Number of projects
Border control	
Surveillance	8
Biometrics	7
Migration	6
Social sciences	4
Ethical dimension	3
Supply chain	3
UAV	3
Law enforcement	2
Applications in satellite navigation	1
Blockchain	1
Cloud	1
Disaster management	1
Forensics	1
IoT	1
Rescue	1
Transport	1
CBRN-E	
Forensics	2
Law enforcement	2
Certification	1
Emergency	1
Rescue	1
Standardisation	1
Supply chain	1
Transport	1
Combating radicalisation	
Social sciences	12
Social media	7
Violence	7
Law enforcement	4
Ethical dimension	1
Migration	1

Building block / Main focus	Number of projects
Critical infrastructures	
Surveillance	9
UAV	9
ICT	8
Physical threats	8
Resilience	7
Disaster management	6
CPS	4
Emergency	4
Transport	4
Law enforcement	3
Preparedness	2
Biometrics	1
Certification	1
Cloud	1
Cryptography	1
IoT	1
Privacy	1
Rescue	1
Standardisation	1
Supply chain	1
Supply security	1
Critical supplies	
Supply security	2
Cybersecurity	
Cryptography	31
ICT	31
Privacy	26
IoT	22
Cloud	21
Biometrics	12
CPS	7
Physical threats	6
Social sciences	5

Building block / Main focus	Number of projects
Blockchain	4
Law enforcement	4
Social media	4
Transport	4
Applications in satellite navigation	3
Certification	2
Ethical dimension	2
Forensics	2
Preparedness	2
Standardisation	2
Supply chain	2
Disaster management	1
Information exchange	1
Resilience	1
Training	1
Violence	1
Defence	
External security	9
Peace keeping	5
Social sciences	3
Training	2
Information exchange	1
Violence	1
Hybrid threats	
ICT	1
Physical threats	1
Social media	1
Transport	1
Public spaces/Soft targets	
UAV	8
Emergency	7
Surveillance	6
Disaster management	5
Law enforcement	4

Building block / Main focus	Number of projects
Biometrics	3
Transport	3
Applications in satellite navigation	2
Preparedness	2
Certification	1
Forensics	1
ICT	2
Physical threats	1
Privacy	1
Rescue	1
Resilience	1
Social sciences	1
Standardisation	1
Violence	1
Space	
Applications in satellite navigation	8
Surveillance	3
Transport	3
UAV	3
Rescue	2
Migration	1
Standardisation	1
Terrorism financing	
Law enforcement	4
Forensics	2
Social media	1
Social sciences	1
Other (outside of building blocks)	
Law enforcement	22
Forensics	10
Social sciences	9
Surveillance	5
Emergency	4
Biometrics	3

Building block / Main focus	Number of projects
Disaster management	3
UAV	3
Ethical dimension	2
External security	2
ICT	3
IoT	2
Migration	2
Rescue	2
Training	2
Certification	1
Information exchange	1
Peace keeping	1
Resilience	1
Social media	1
Standardisation	1

Source: JRC analysis of Cordis data.

Table 19: Number of projects by priority and main focus

Priority / Main focus	Number of projects
Cybercrime	
ICT	33
Cryptography	31
Privacy	26
IoT	23
Cloud	21
Biometrics	12
CPS	7
Physical threats	6
Law enforcement	5
Social sciences	5
Blockchain	4
Social media	4
Transport	4
Applications in satellite navigation	3
Certification	2

Priority / Main focus	Number of projects
Ethical dimension	2
Forensics	2
Preparedness	2
Standardisation	2
Supply chain	2
Training	2
Disaster management	1
Information exchange	1
Resilience	1
Violence	1
Organised crime	
Law enforcement	18
Social sciences	10
Forensics	9
Surveillance	7
Migration	5
Biometrics	3
Supply chain	3
UAV	2
Applications in satellite navigation	1
Cloud	1
Ethical dimension	1
External security	1
IoT	1
Training	1
Terrorism and radicalisation	
Law enforcement	19
Social sciences	14
Surveillance	12
UAV	10
Disaster management	8
Resilience	8
Social media	8
Violence	8

Priority / Main focus	Number of projects
Biometrics	7
Emergency	7
Transport	6
Forensics	5
ICT	5
Physical threats	4
Ethical dimension	3
Applications in satellite navigation	2
Migration	2
Preparedness	2
Rescue	2
Standardisation	2
Training	2
Blockchain	1
Certification	1
Cloud	1
External security	1
Privacy	1
Supply chain	1
Supply security	1

Source: JRC analysis of Cordis data.

Table 20: Number of projects funded under Programme 3.7 and under other programmes

	Funded under 3.7	Funded under other programmes
Programme 3.7	103	
Programmes 3.7 & 2	100	
Programmes 3.7 & 3.1	2	
Programme 1		68
Programme 2		54
Programmes 2 & 3		10
Programme 3		9
Programme 4		3

Source: JRC analysis of Cordis data.

Table 21: Number of projects per H2020 funding programme

H2020 Programme	Number of projects
1.1.	36
1.2.1.	1
1.3.1.	2
1.3.2.	25
1.3.3.	4
2	3
2.1.1.	45
2.1.1.1.	1
2.1.1.3.	7
2.1.1.6.	1
2.1.2.	1
2.1.6.	6
2.1.6.1.2.	3
2.1.6.3.	3
2.3.1.	114
2.3.2.2.	2
3	3
3.1.	2
3.2.1.	1
3.2.5.	1
3.4.	2
3.4.1.2.	2
3.4.2.2.	2
3.4.7.	3
3.4.8.2.	1
3.5.	1
3.5.3.	2
3.6.	2
3.6.1.2.	1
3.7.	163
3.7.1.	16
3.7.2.	8
3.7.3.	8
3.7.4.	19
3.7.5.	9
3.7.6.	16
3.7.7.	10
3.7.8.	7
4.a.	3

Source: JRC analysis of Cordis data.

Table 22: Distribution of projects by building block and funding programme

	H2020 funding programme	
	3.7	Non-3.7
Building block	Number of projects	
Cybersecurity	87	80
Critical infrastructures	60	8
Public spaces	37	6
Border control	27	12
CBRN-E	20	4
Combating radicalisation	9	9
Space		10
Defence*	6	3
Terrorism financing*	5	2
Hybrid threats*	1	2
Critical supplies*		2
Others (outside building blocks)	28	20
All projects	205	144

Note: *Building blocks with fewer than 10 projects.

Source: JRC analysis of Cordis data.

Table 23: Number of projects to which countries contribute

	Role in the project		
Country	Coordinator	Participant	Total
EU Member States			
UK	48	204	252
ES	51	188	239
IT	40	191	231
DE	22	195	217
FR	31	153	184
EL	12	114	126
BE	16	94	110
NL	25	74	99
PT	10	60	70
AT	17	49	66
FI	8	46	54

	Role in the project		
Country	Coordinator	Participant	Total
PL	6	47	53
IE	8	44	52
RO	1	41	42
SE	3	31	34
DK	7	22	29
LU	1	16	17
BG	1	15	16
CY	4	12	16
CZ	3	13	16
EE	1	14	15
HU	1	13	14
SI	0	12	12
SK	2	6	8
MT	1	6	7
LV	1	5	6
HR	0	4	4
LT	0	2	2
Other countries			
IL	12	41	53
CH	3	40	43
NO	11	28	39
TR	2	7	9
RS	0	6	6
ZA	0	5	5
US	0	4	4
IS	1	2	3
TN	0	3	3
BA	0	2	2
GE	0	2	2
TH	0	2	2
VN	0	2	2
AL	0	1	1
GI	0	1	1

	Role in the project		
Country	Coordinator	Participant	Total
IN	0	1	1
KR	0	1	1
MD	0	1	1
MK	0	1	1
ML	0	1	1
MY	0	1	1
RU	0	1	1
TW	0	1	1
UA	0	1	1
XK	0	1	1
YE	0	1	1
Total	349	1828	2177

Source: JRC analysis of Cordis data.

Table 24: Number of projects by building block to which countries contribute

Border control	Role in the project		
Country	Coordinator	Participant	Total
EU Member States			
UK	7	19	26
IT	7	16	23
EL	2	17	19
FR	2	17	19
DE	1	17	18
PT	3	13	16
NL	6	8	14
BE	1	11	12
ES	1	11	12
PL	0	11	11
RO	0	10	10
FI	2	5	7
HU	0	6	6
BG	1	4	5
AT	2	2	4
LU	1	3	4
CZ	0	2	2

IE	0	2	2
CY	0	1	1
DK	0	1	1
EE	0	1	1
LV	0	1	1
SE	1	0	1
Other countries			
IL	0	5	5
CH	0	3	3
NO	1	2	3
TR	1	0	1
Total	39	188	227
CBRN-E	Role in the project		
Country	Coordinator	Participant	Total
EU Member States			
IT	4	10	14
UK	3	11	14
DE	1	12	13
FR	1	11	12
FI	2	7	9
BE	4	4	8
IE	2	5	7
NL	4	2	6
PL	0	6	6
ES	1	4	5
SE	0	3	3
CZ	0	2	2
EL	0	2	2
HU	0	2	2
PT	0	1	1
Other countries			
CH	0	3	3
NO	1	2	3
IL	1	0	1
TR	0	1	1
Total	24	88	112

Combating radicalisation	Role in the project		
Country	Coordinator	Participant	Total
EU Member States			
ES	2	20	22
IT	3	18	21
FR	2	17	19
UK	5	14	19
BE	0	13	13
DE	1	12	13
NL	3	9	12
EL	0	8	8
PL	0	7	7
AT	0	5	5
PT	0	5	5
IE	0	4	4
DK	1	1	2
FI	0	1	1
HR	0	1	1
LV	0	1	1
MT	0	1	1
SE	0	1	1
SI	0	1	1
SK	1	0	1
Other countries			
TN	0	3	3
IL	0	2	2
AL	0	1	1
BA	0	1	1
CH	0	1	1
NO	0	1	1
RU	0	1	1
TR	0	1	1
US	0	1	1
Total	18	151	169

Critical infrastructures	Role in the project		
Country	Coordinator	Participant	Total
EU Member States			
IT	10	40	50
DE	7	38	45
ES	14	28	42
UK	6	33	39
FR	6	20	26
EL	3	22	25
BE	3	11	14
NL	3	10	13
IE	2	10	12
PT	1	11	12
SE	1	8	9
AT	2	6	8
LU	0	6	6
PL	1	5	6
RO	0	6	6
DK	2	3	5
SI	0	5	5
HU	1	2	3
CY	2	0	2
FI	0	2	2
CZ	0	1	1
EE	0	1	1
LV	0	1	1
SK	1	0	1
Other countries			
IL	0	12	12
NO	3	9	12
CH	0	3	3
RS	0	1	1
Total	68	294	362

Critical supplies	Role in the project		
Country	Coordinator	Participant	Total
EU Member States			
DE	2	4	6
ES	0	5	5
FI	0	4	4
SE	0	2	2
UK	0	2	2
FR	0	1	1
IT	0	1	1
Other countries			
ZA	0	3	3
Total	2	22	24
Cybersecurity	Role in the project		
Country	Coordinator	Participant	Total
EU Member States			
ES	28	89	117
UK	20	93	113
IT	14	98	112
DE	10	94	104
FR	19	72	91
EL	7	65	72
BE	7	41	48
AT	13	25	38
NL	4	31	35
PT	5	20	25
FI	2	16	18
DK	3	13	16
SE	1	15	16
IE	3	12	15
RO	0	14	14
LU	0	11	11
PL	4	6	10
EE	1	8	9
SI	0	9	9

CY	1	7	8
CZ	2	6	8
BG	0	3	3
MT	1	2	3
HU	1	1	2
LV	1	0	1
SK	0	1	1
Other countries			
CH	2	32	34
IL	9	21	30
NO	7	6	13
US	0	4	4
RS	0	2	2
TH	0	2	2
TR	1	1	2
VN	0	2	2
GE	0	1	1
GI	0	1	1
IN	0	1	1
IS	1	0	1
KR	0	1	1
MY	0	1	1
TW	0	1	1
ZA	0	1	1
Total	169	829	998
Defence	Role in the project		
Country	Coordinator	Participant	Total
EU Member States			
UK	3	8	11
NL	1	6	7
FI	1	5	6
IE	1	5	6
ES	1	4	5
AT	1	3	4
DE	0	4	4

DK	0	4	4
BE	0	3	3
IT	1	2	3
PL	0	2	2
SI	0	2	2
BG	0	1	1
EE	0	1	1
FR	0	1	1
PT	0	1	1
RO	0	1	1
Other countries			
GE	0	1	1
ML	0	1	1
RS	0	1	1
UA	0	1	1
XK	0	1	1
YE	0	1	1
Total	9	59	68
Hybrid threats	Role in the project		
Country	Coordinator	Participant	Total
EU Member States			
ES	1	7	8
FR	0	4	4
IT	1	3	4
EL	0	3	3
BE	0	2	2
AT	0	1	1
DE	0	1	1
IE	0	1	1
PT	1	0	1
SE	0	1	1
SI	0	1	1
UK	0	1	1
Total	3	25	28

Public spaces/Soft targets	Role in the project		
Country	Coordinator	Participant	Total
EU Member States			
ES	10	14	24
UK	7	12	19
IT	5	11	16
DE	2	9	11
NL	4	7	11
FR	2	7	9
BE	2	3	5
EL	1	4	5
PL	1	4	5
IE	0	4	4
PT	1	3	4
AT	2	1	3
DK	2	1	3
RO	0	2	2
SE	1	1	2
BG	0	1	1
CY	1	0	1
CZ	1	0	1
FI	0	1	1
HR	0	1	1
Other countries			
IL	0	2	2
NO	1	1	2
BA	0	1	1
TR	0	1	1
Total	43	91	134
Space	Role in the project		
Country	Coordinator	Participant	Total
EU Member States			
ES	4	6	10
IT	3	6	9
DE	1	6	7

UK	1	4	5
FR	1	2	3
NL	0	3	3
FI	0	2	2
PL	0	2	2
AT	0	1	1
IE	0	1	1
BE	0	1	1
DK	0	1	1
EL	0	1	1
SE	0	1	1
Other countries			
IN	0	1	1
KR	0	1	1
Total	10	39	49
Terrorism financing	Role in the project		
Country	Coordinator	Participant	Total
EU Member States			
ES	1	10	11
DE	1	7	8
UK	1	6	7
IT	1	5	6
AT	1	3	4
NL	1	3	4
BE	0	2	2
FR	0	2	2
PT	0	2	2
EL	0	1	1
FI	0	1	1
IE	0	1	1
Other countries			
NO	1	0	1
Total	7	43	50

Other (outside building blocks)	Role in the project		Total
	Coordinator	Participant	
Country			
EU Member States			
ES	6	37	43
IT	6	34	40
UK	4	37	41
DE	2	34	36
FR	6	26	32
BE	3	21	24
NL	6	17	23
PT	2	13	15
RO	1	14	15
EL	2	12	14
AT	1	12	13
PL	1	12	13
FI	2	6	8
SE	0	8	8
BG	0	6	6
IE	0	6	6
SK	0	5	5
CY	0	4	4
CZ	0	4	4
EE	0	4	4
HU	0	4	4
MT	0	3	3
HR	0	2	2
LT	0	2	2
LU	0	2	2
LV	0	2	2
SI	0	1	1
Other countries			
NO	2	12	14
IL	2	10	12
TR	0	3	3
CH	1	1	2

IS	0	2	2
RS	0	2	2
DK	1	0	1
MD	0	1	1
MK	0	1	1
ZA	0	1	1
Total	48	361	409

Source: JRC analysis of Cordis data.

Table 25: Number of contributing organisations by legal status

Legal status	Number of organisations
Private for-profit entities	645
Higher and secondary education establishments	296
Research organisations	178
Public bodies	163
Others	66

Source: JRC analysis of Cordis data.

Table 26 Number of contributions from organisations by legal status and role

All projects	Role in the project		
Legal status	Coordinator	Participant	Total
Private for-profit entities	189	702	891
Higher or secondary education establishments	95	454	549
Research organisations	54	313	367
Public bodies	8	300	308
Others	3	72	75
Total	349	1841	2190

Source: JRC analysis of Cordis data.

Table 27: Number of contributions from organisations by building block, legal status and role

Border control	Role in the project		
Legal status	Coordinator	Participant	Total
Private for-profit entities	26	76	102
Public bodies	0	47	47
Higher or secondary education establishments	9	32	41
Research organisations	4	29	33
Other	0	4	4
Total	39	188	227

CBRN-E	Role in the project		
Legal status	Coordinator	Participant	Total
Private for-profit entities	14	28	42
Higher or secondary education establishments	5	23	28
Research organisations	4	20	24
Public bodies	1	16	17
Other	0	1	1
Total	24	88	112
Combating radicalisation	Role in the project		
Legal status	Coordinator	Participant	Total
Higher or secondary education establishments	11	46	57
Public bodies	2	45	47
Private for-profit entities	2	30	32
Research organisations	3	20	23
Other	0	10	10
Total	18	151	169
Critical infrastructures	Role in the project		
Legal status	Coordinator	Participant	Total
Private for-profit entities	51	140	191
Research organisations	10	53	63
Higher or secondary education establishments	7	55	62
Public bodies	0	37	37
Other	0	9	9
Total	68	294	362
Critical supplies	Role in the project		
Legal status	Coordinator	Participant	Total
Private for-profit entities	0	12	12
Research organisations	2	3	5
Higher or secondary education establishments	0	4	4
Other	0	2	2
Public bodies	0	1	1
Total	2	22	24
Cybersecurity	Role in the project		
Legal status	Coordinator	Participant	Total
Private for-profit entities	95	413	508
Higher or secondary education establishments	41	209	250
Research organisations	30	135	165
Public bodies	1	50	51
Other	0	22	22
Total	167	829	996

Defence	Role in the project		
Legal status	Coordinator	Participant	Total
Higher or secondary education establishments	6	25	31
Research organisations	0	12	12
Private for-profit entities	2	9	11
Public bodies	0	8	8
Other	1	5	6
Total	9	59	68
Hybrid threats	Role in the project		
Legal status	Coordinator	Participant	Total
Private for-profit entities	2	13	15
Research organisations	1	4	5
Higher or secondary education establishments	0	4	4
Other	0	3	3
Public bodies	0	1	1
Total	3	25	28
Public spaces/Soft targets	Role in the project		
Legal status	Coordinator	Participant	Total
Private for-profit entities	37	32	69
Public bodies	0	31	31
Higher or secondary education establishments	2	15	17
Research organisations	3	11	14
Other	1	2	3
Total	43	91	134
Space	Role in the project		
Legal status	Coordinator	Participant	Total
Private for-profit entities	8	15	23
Research organisations	1	10	11
Higher or secondary education establishments	0	11	11
Public bodies	1	3	4
Total	10	39	49
Terrorism financing	Role in the project		
Legal status	Coordinator	Participant	Total
Private for-profit entities	4	15	19
Public bodies	0	12	12
Higher or secondary education establishments	2	9	11
Research organisations	1	7	8
Total	7	43	50

Other (outside building blocks)	Role in the project		
Legal status	Coordinator	Participant	Total
Private for-profit entities	19	89	108
Public bodies	3	99	102
Higher or secondary education establishments	17	83	100
Research organisations	8	68	76
Other	1	22	23
Total	48	361	409

Source: JRC analysis of Cordis data.

Table 28: Number of contributions from organisations by priority, legal status and role

Priority: Cybercrime	Role in the project		
Legal status	Coordinator	Participant	Total
Private for-profit entities	97	419	516
Higher or secondary education establishments	41	214	255
Research organisations	30	138	168
Public bodies	1	53	54
Other	0	23	23
Total	169	847	1016
Priority: Organised crime	Role in the project		
Legal status	Coordinator	Participant	Total
Private for-profit entities	23	103	126
Higher or secondary education establishments	15	75	90
Public bodies	1	87	88
Research organisations	7	49	56
Other	0	13	13
Total	46	327	373
Priority: Terrorism and radicalisation	Role in the project		
Legal status	Coordinator	Participant	Total
Private for-profit entities	76	196	272
Higher or secondary education establishments	26	154	180
Public bodies	3	141	144
Research organisations	15	110	125
Other	0	31	31
Total	120	632	752

Source: JRC analysis of Cordis data.

Table 29: Number of projects with dual-use potential

Dual use	Number of projects
Yes	311
No	38
Total	349

Source: JRC analysis of Cordis data

Table 30: Number of projects by priority and dual-use potential

	Priority			
Dual use	Cybercrime	Terrorism	Organised crime	Outside priorities
Yes	161	110	34	37
No	8	10	12	12
Total	169	120	46	49

Source: JRC analysis of Cordis data.

Table 31: Number of projects by building block and dual-use potential

	Dual use	
Building block	Yes	No
Cybersecurity	159	8
Critical infrastructures	68	
Public spaces	43	
Border control	32	7
CBRN-E	24	
Combating radicalisation	12	6
Space	10	
Defence*	8	1
Terrorism financing*	5	2
Hybrid threats*	3	
Critical supplies*	2	
Other (outside building blocks)	33	15

Note: *Building blocks with fewer than 10 projects.

Source: JRC analysis of Cordis data.

Annex 6. Entities participating in H2020 security- and defence-related projects

Abbreviations used for "Legal status":

HES: Higher or secondary education establishments

REC: Research organisations

PRC: Private for-profit entities (excluding higher or secondary education establishments)

PUB: Public bodies (excluding research organisations and higher or secondary education establishments)

OTH: Other

Table 32: Entities participating in at least 2 projects related to "Border control"

Name of entity	Legal status	Country	Number of projects
FRAUNHOFER GESELLSCHAFT ZUR FOERDERUNG DER ANGEWANDTEN FORSCHUNG E.V.	REC	DE	4
INSPECTORATUL GENERAL AL POLITIEI DE FRONTIERA	PUB	RO	4
MINISTRY OF NATIONAL DEFENCE, GREECE	PUB	EL	3
ORSZAGOS RENDOR - FOKAPITANYSAG	PUB	HU	3
NATO SCIENCE AND TECHNOLOGY ORGANISATION	REC	BE	3
SERVICIUL DE PROTECTIE SI PAZA	PUB	RO	3
ATOS SPAIN SA	PRC	ES	3
MINISTERIO DA ADMINISTRACAO INTERNA	PUB	PT	3
KENTRO MELETON ASFALIAS	REC	EL	3
UNIVERSITE DE NAMUR ASBL	HES	BE	2
MINISTERIO DA DEFESA NACIONAL	PUB	PT	2
INSTITUT PO OTBRANA	REC	BG	2
AUDAX GLOBAL SOLUTIONS LIMITED	PRC	UK	2
NEDERLANDSE ORGANISATIE VOOR TOEGEPAST NATUURWETENSCHAPPELIJK ONDERZOEK TNO	REC	NL	2
COMMISSARIAT A L'ENERGIE ATOMIQUE ET AUX ENERGIES ALTERNATIVES	REC	FR	2
AGENZIA DELLE DOGANE	PUB	IT	2
ENGINEERING - INGEGNERIA INFORMATICA SPA	PRC	IT	2
ITTI SP ZOO	PRC	PL	2
ETHNIKO KENTRO EREVNAS KAI TECHNOLOGIKIS ANAPTYXIS	REC	EL	2
MINISTERIO DEL INTERIOR	PUB	ES	2
EXODUS ANONYMOS ETAIREIA PLIROFORIKIS	PRC	EL	2
TEKNOLOGIAN TUTKIMUSKESKUS VTT OY	REC	FI	2
HOME OFFICE	PUB	UK	2
UNIVERSITEIT VAN AMSTERDAM	HES	NL	2
INOV INESC INOVACAO - INSTITUTO DE NOVAS TECNOLOGIAS	REC	PT	2
KOMENDA GLOWNA STRAZY GRANICZNEJ	PUB	PL	2

Source: JRC analysis of Cordis data.

Table 33: Entities participating in at least 2 projects related to "CBRN-E"

Name of entity	Legal status	Country	Number of projects
JRC -JOINT RESEARCH CENTRE- EUROPEAN COMMISSION	REC	BE	4
HELSINGIN YLIOPISTO	HES	FI	2
ENVIRONICS OY	PRC	FI	2
UNIVERSITE CATHOLIQUE DE LOUVAIN	HES	BE	2
COMMISSARIAT A L'ENERGIE ATOMIQUE ET AUX ENERGIES ALTERNATIVES	REC	FR	2
UNIVERSITAET PADERBORN	HES	DE	2

Source: JRC analysis of Cordis data.

Table 34: Entities participating in at least 2 projects related to "Combating radicalisation"

Name of entity	Legal status	Country	Number of projects
AYUNTAMIENTO DE MADRID	PUB	ES	4
KENTRO MELETON ASFALIAS	REC	EL	4
EUROPEAN ORGANISATION FOR SECURITY SCRL	PRC	BE	3
POLICE SERVICE OF NORTHERN IRELAND	PUB	UK	3
MINISTERIO DEL INTERIOR	PUB	ES	3
THE UNIVERSITY OF WARWICK	HES	UK	2
EXPERT SYSTEM IBERIA SL	PRC	ES	2
ETHNIKO KENTRO EREVNAS KAI TECHNOLOGIKIS ANAPTYXIS	REC	EL	2
MINISTERO DELL'INTERNO	PUB	IT	2
FORUM EUROPEEN POUR LA SECURITE URBAINE	OTH	FR	2
NEDERLANDSE ORGANISATIE VOOR TOEGEPAST NATUURWETENSCHAPPELIJK ONDERZOEK TNO	REC	NL	2
FRAUNHOFER GESELLSCHAFT ZUR FOERDERUNG DER ANGEWANDTEN FORSCHUNG E.V.	REC	DE	2
SHEFFIELD HALLAM UNIVERSITY	HES	UK	2
HOCHSCHULE FUR DEN OFFENTLICHEN DIENST IN BAYERN	HES	DE	2
UNIVERSITA CATTOLICA DEL SACRO CUORE	HES	IT	2
UNIVERSITEIT UTRECHT	HES	NL	2
MINISTERIO DA JUSTICA	PUB	PT	2
MINISTERO DELLA GIUSTIZIA	PUB	IT	2

Source: JRC analysis of Cordis data.

Table 35: Entities participating in at least 2 projects related to "Critical infrastructures"

Name of entity	Legal status	Country	Number of projects
FRAUNHOFER GESELLSCHAFT ZUR FOERDERUNG DER ANGEWANDTEN FORSCHUNG E.V.	REC	DE	6
ATOS SPAIN SA	PRC	ES	4

Name of entity	Legal status	Country	Number of projects
STIFTELSEN SINTEF	REC	NO	4
KATHOLIEKE UNIVERSITEIT LEUVEN	HES	BE	3
JRC -JOINT RESEARCH CENTRE- EUROPEAN COMMISSION	REC	BE	3
MINISTERO DELL'INTERNO	PUB	IT	3
ENGINEERING - INGEGNERIA INFORMATICA SPA	PRC	IT	3
TECHNISCHE UNIVERSITAET BRAUNSCHWEIG	HES	DE	3
IMPERIAL COLLEGE OF SCIENCE TECHNOLOGY AND MEDICINE	HES	UK	3
UNIVERSITY OF PIRAEUS RESEARCH CENTER	HES	EL	3
SINGULARLOGIC ANONYMI ETAIREIA PLIROFORIAKON SYSTIMATON KAI EFARMOGON PLIROFORIKIS	PRC	EL	2
ONTECH SECURITY SL	PRC	ES	2
TECHNISCHE UNIVERSITEIT EINDHOVEN	HES	NL	2
FUNDACION DE LA COMUNIDAD VALENCIANA PARA LA INVESTIGACION, PROMOCION Y ESTUDIOS COMERCIALES DE VALENCIAPORT	REC	ES	2
RHEINISCH-WESTFAELISCHE TECHNISCHE HOCHSCHULE AACHEN	HES	DE	2
AEORUM ESPANA S.L.	PRC	ES	2
AIT AUSTRIAN INSTITUTE OF TECHNOLOGY GMBH	REC	AT	2
INOV INESC INOVACAO - INSTITUTO DE NOVAS TECNOLOGIAS	REC	PT	2
MYDEFENCE COMMUNICATION APS	PRC	DK	2
THALES SA	PRC	FR	2
PIRAEUS PORT AUTHORITY SA	PRC	EL	2
UNIVERSITE DU LUXEMBOURG	HES	LU	2

Source: JRC analysis of Cordis data.

Table 36: Entities participating in projects related to "Critical supplies"

Name of entity	Legal status	Country	Number of projects
OEKO-INSTITUT E.V. - INSTITUT FUER ANGEWANDTE OEKOLOGIE	REC	DE	1
UNIVERSITY OF THE WITWATERSRAND JOHANNESBURG	HES	ZA	1
SRK EXPLORATION SERVICES LIMITED	PRC	UK	1
AARHUS GEOFISICA SRL	PRC	IT	1
HELMHOLTZ-ZENTRUM DRESDEN-ROSSENDORF EV	REC	DE	1
AGENCIA DE INNOVACION Y DESARROLLO DE ANDALUCIA	PUB	ES	1
PROJEKT-CONSULT BERATUNG IN ENTWICKLUNGSLANDERN GMBH	PRC	DE	1
ASISTENCIAS TECNICAS CLAVE SL	PRC	ES	1
SUPRACON AG	PRC	DE	1
ATALAYA RIO TINTO MINERA SL	PRC	ES	1
GEORANGE IDEELLA FORENING	OTH	SE	1
COBRE LAS CRUCES SA	PRC	ES	1
ITA-SUOMEN YLIOPISTO	HES	FI	1

Name of entity	Legal status	Country	Number of projects
DIALOGIK GEMEINNUETZIGE GESELLSCHAFT FUER KOMMUNIKATIONS- UND KOOPERATIONSFORSCHUNG mbH	REC	DE	1
OULUN YLIOPISTO	HES	FI	1
DMT-KAI BATLA PTY LTD	PRC	ZA	1
SNL FINANCIAL SWEDEN AB	PRC	SE	1
FEDERATION EUROPEENNE DES GEOLOGUES	OTH	FR	1
SUOMEN YMPARISTOKESKUS	REC	FI	1
FRAUNHOFER GESELLSCHAFT ZUR FOERDERUNG DER ANGEWANDTEN FORSCHUNG E.V.	REC	DE	1
UNIVERSITY OF DUNDEE	HES	UK	1
GALSA (PTY) LTD	PRC	ZA	1
AA SAKATTI MINING OY	PRC	FI	1
GEOGNOSIA SLL	PRC	ES	1

Source: JRC analysis of Cordis data.

Table 37: Entities participating in at least 4 projects related to "Cybersecurity"

Name of entity	Legal status	Country	Number of projects
ATOS SPAIN SA	PRC	ES	19
KATHOLIEKE UNIVERSITEIT LEUVEN	HES	BE	16
INSTITUT NATIONAL DE RECHERCHE ENINFORMATIQUE ET AUTOMATIQUE	REC	FR	11
RUHR-UNIVERSITAET BOCHUM	HES	DE	9
FRAUNHOFER GESELLSCHAFT ZUR FOERDERUNG DER ANGEWANDTEN FORSCHUNG E.V.	REC	DE	8
IBM RESEARCH GMBH	PRC	CH	8
TECHNISCHE UNIVERSITAT DARMSTADT	HES	DE	7
IBM ISRAEL - SCIENCE AND TECHNOLOGY LTD	PRC	IL	7
AIT AUSTRIAN INSTITUTE OF TECHNOLOGY GMBH	REC	AT	7
THALES COMMUNICATIONS & SECURITY SAS	PRC	FR	6
TECHNIKON FORSCHUNGS- UND PLANUNGSGESELLSCHAFT MBH	PRC	AT	6
UNIVERSITY OF PIRAEUS RESEARCH CENTER	HES	EL	6
UNIVERSITY OF SOUTHAMPTON	HES	UK	6
IMPERIAL COLLEGE OF SCIENCE TECHNOLOGY AND MEDICINE	HES	UK	6
FOUNDATION FOR RESEARCH AND TECHNOLOGY HELLAS	REC	EL	6
XLAB RAZVOJ PROGRAMSKE OPREME IN SVETOVANJE DOO	PRC	SI	5
TRUST-IT SERVICES LIMITED	PRC	UK	5
TECHNISCHE UNIVERSITAET GRAZ	HES	AT	5
TECHNISCHE UNIVERSITEIT EINDHOVEN	HES	NL	5
CONSIGLIO NAZIONALE DELLE RICERCHE	REC	IT	5
COMMISSARIAT A L'ENERGIE ATOMIQUE ET AUX ENERGIES ALTERNATIVES	REC	FR	5

Name of entity	Legal status	Country	Number of projects
ENGINEERING - INGEGNERIA INFORMATICA SPA	PRC	IT	5
UNIVERSITY COLLEGE LONDON	HES	UK	4
MONTIMAGE EURL	PRC	FR	4
UNIVERSITY OF BRISTOL	HES	UK	4
THE CHANCELLOR, MASTERS AND SCHOLARS OF THE UNIVERSITY OF OXFORD	HES	UK	4
THALES SERVICES SAS	PRC	FR	4
ROYAL HOLLOWAY AND BEDFORD NEW COLLEGE	HES	UK	4
TELEFONICA INVESTIGACION Y DESARROLLO SA	PRC	ES	4
TECHNISCHE UNIVERSITAET BRAUNSCHWEIG	HES	DE	4
IDEMIA IDENTITY & SECURITY FRANCE	PRC	FR	4
FUNDACION TECNALIA RESEARCH & INNOVATION	REC	ES	4
INSTITUTE OF COMMUNICATION AND COMPUTER SYSTEMS	REC	EL	4
FONDAZIONE CENTRO SAN RAFFAELE	REC	IT	4
ETHNIKO KENTRO EREVNAS KAI TECHNOLOGIKIS ANAPTYXIS	REC	EL	4

Source: JRC analysis of Cordis data.

Table 38: Entities participating in at least 2 projects related to "Defence"

Name of entity	Legal status	Country	Number of projects
UNIVERSITY OF BRISTOL	HES	UK	2
NATIONAL UNIVERSITY OF IRELAND MAYNOOTH	HES	IE	2
NATIONAL DEFENCE UNIVERSITY	HES	FI	2
EUROPEAN UNION SATELLITE CENTRE	PUB	ES	2
ROSKILDE UNIVERSITET	HES	DK	2
FORSVARET OG FORSVARSMINISTERIETS STYRELSE	PUB	DK	2
ISTITUTO AFFARI INTERNAZIONALI	REC	IT	2
LAUREA-AMMATTIKORKEAKOULU OY	HES	FI	2

Source: JRC analysis of Cordis data.

Table 39: Entities participating in projects related to "Hybrid threats"

Name of entity	Legal status	Country	Number of projects
INNOVASEC LTD	PRC	UK	1
THALES SA	PRC	FR	1
NOATUM PORTS VALENCIANA, S.A.U.	PRC	ES	1
AIT AUSTRIAN INSTITUTE OF TECHNOLOGY GMBH	REC	AT	1
UNIVERSITY OF PIRAEUS RESEARCH CENTER	HES	EL	1
ATSEC INFORMATION SECURITY AB	PRC	SE	1
LIVE TECH SRL	PRC	IT	1
AUTORITA DI SISTEMA PORTUALE DEL MAR TIRRENO SETTENTRIONALE	PUB	IT	1

Name of entity	Legal status	Country	Number of projects
S2 GRUPO DE INNOVACION EN PROCESOS ORGANIZATIVOS SL	PRC	ES	1
CASSIDIAN CYBERSECURITY SAS	PRC	FR	1
UNIVERSIDAD POLITECNICA DE MADRID	HES	ES	1
DE VLAAMSE RADIO EN TELEVISIEOMROEPORGANISATIE NV	OTH	BE	1
IDEMIA IDENTITY & SECURITY FRANCE	PRC	FR	1
ENGINEERING - INGEGNERIA INFORMATICA SPA	PRC	IT	1
KATHOLIEKE UNIVERSITEIT LEUVEN	HES	BE	1
ETHNIKO KENTRO EREVNAS KAI TECHNOLOGIKIS ANAPTYXIS	REC	EL	1
LUKA KOPER, PORT AND LOGISTIC SYSTEM, D.D.	PRC	SI	1
ETRA INVESTIGACION Y DESARROLLO SA	PRC	ES	1
PIRAEUS PORT AUTHORITY SA	PRC	EL	1
EVOLEO TECHNOLOGIES LDA	PRC	PT	1
SINDICE LIMITED	PRC	IE	1
FORTISS GMBH	REC	DE	1
UNION INTERNATIONALE DES CHEMINS DE FER	OTH	FR	1
FUNDACION CIUDADANA CIVIO	OTH	ES	1
UNIVERSITAT POLITECNICA DE VALENCIA	HES	ES	1
FUNDACION DE LA COMUNIDAD VALENCIANA PARA LA INVESTIGACION, PROMOCION Y ESTUDIOS COMERCIALES DE VALENCIAPORT	REC	ES	1
AGENZIA ANSA - AGENZIA NAZIONALE STAMPA ASSOCIATA - SOCIETA COOPERATIVA	PRC	IT	1
FUNDACIÓN INVESTIGACIÓN UNIVERSIDAD EMPRESA JAKINTZA LANEZKO IKERKUNTZA - EUSKOIKER	REC	ES	1

Source: JRC analysis of Cordis data.

Table 40 Entities participating in at least 2 projects related to "Public spaces"

Name of entity	Legal status	Country	Number of projects
MINISTERO DELL'INTERNO	PUB	IT	3
MINISTERIO DA ADMINISTRACAO INTERNA	PUB	PT	2
PROPRS Ltd.	PRC	UK	2
AUDAX GLOBAL SOLUTIONS LIMITED	PRC	UK	2
MINISTERIO DEL INTERIOR	PUB	ES	2
DEEP BLUE SRL	PRC	IT	2
MYDEFENCE COMMUNICATION APS	PRC	DK	2
DEUTSCHES ZENTRUM FUER LUFT - UND RAUMFAHRT EV	REC	DE	2
AEORUM ESPANA S.L.	PRC	ES	2
UNIVERSITY OF LEEDS	HES	UK	2

Source: JRC analysis of Cordis data.

Table 41: Entities participating in projects related to "Space"

Name of entity	Legal status	Country	Number of projects
EUROPEAN UNION SATELLITE CENTRE	PUB	ES	2
SATELLITE APPLICATIONS CATAPULT LIMITED	REC	UK	1
ISTITUTO SUPERIORE MARIO BOELLA SULLE TECNOLOGIE DELL'INFORMAZIONE E DELLE TELECOMUNICAZIONI ASSOCIAZIONE	REC	IT	1
AGENCIA ESTATAL CONSEJO SUPERIOR DEINVESTIGACIONES CIENTIFICAS	REC	ES	1
AGENZIA SPAZIALE ITALIANA	REC	IT	1
NOTTINGHAM SCIENTIFIC LTD	PRC	UK	1
AGIT AACHENER GESELLSCHAFT FUR INNOVATION UND TECHNOLOGIETRANSFER MITBESCHRANKTER HAFTUNG	PRC	DE	1
TELECONSULT AUSTRIA GMBH	PRC	AT	1
AKADEMIA MORSKA W SZCZECINIE AM	HES	PL	1
UNIVERSITA DEGLI STUDI DI ROMA LA SAPIENZA	HES	IT	1
ARATOS SYSTEMS BV	PRC	NL	1
NAVCERT GMBH	PRC	DE	1
ASOCIACION CENTRO TECNOLÓGICO CEIT-IK4	REC	ES	1
ORBITAL SISTEMAS AEROSPAZIALES SL	PRC	ES	1
ASTER SPA	PRC	IT	1
SISTEMATICA SPA	PRC	IT	1
BUSINESS INTEGRATION PARTNERS BELGIUM	PRC	BE	1
THE UNIVERSITY OF BIRMINGHAM	HES	UK	1
CENTRE NATIONAL D'ETUDES SPATIALES - CNES	REC	FR	1
UNIVERSIDAD DE SEVILLA	HES	ES	1
CENTRO PARA EL DESARROLLO TECNOLÓGICO INDUSTRIAL	PUB	ES	1
WATERFORD INSTITUTE OF TECHNOLOGY	HES	IE	1
CHANNARAYAPATNA SHIVARAMAIAH NAGARAJ	PRC	IN	1
MAANMITTAUSLAITOS	REC	FI	1
CRANFIELD UNIVERSITY	HES	UK	1
NAVPOS SYSTEMS GMBH	PRC	DE	1
DAIMLER AG	PRC	DE	1
NOVACOM SERVICES SA	PRC	FR	1
DELFT DYNAMICS B.V.	PRC	NL	1
RINA CONSULTING SPA	PRC	IT	1
DEUTSCHES ZENTRUM FÜR LUFT - UND RAUMFAHRT EV	REC	DE	1
SATWAYS - PROIONTA KAI YPIRESIES TILEMATIKIS DIKTYAKON KAI TILEPIKINONIAKON EFARMOGON ETAIRIA PERIORISMENIS EFTHINIS EPE	PRC	EL	1
ELECTRONICS AND TELECOMMUNICATIONS RESEARCH INSTITUTE	REC	KR	1
STMICROELECTRONICS SRL	PRC	IT	1
ELETTRONICA GMBH	PRC	DE	1

Name of entity	Legal status	Country	Number of projects
THE MAIN SCHOOL OF FIRE SERVICE	HES	PL	1
EURODEV BV	PRC	NL	1
TOPVIEW SRL START UP INNOVATIVA	PRC	IT	1
TOTALFORSVARETS FORSKNINGSINSTITUT	REC	SE	1
TTY-SAATIO	HES	FI	1
UK SPACE AGENCY	PUB	UK	1
EVERIS AEROESPACIAL Y DEFENSA SL	PRC	ES	1
UNIVERSITA DEGLI STUDI DI FIRENZE	HES	IT	1
FRANCE DEVELOPPEMENT CONSEIL (FDC) SARL	PRC	FR	1
UNIVERSITAET STUTTGART	HES	DE	1
FUNDACION CENTRO DE TECNOLOGIAS DE INTERACCION VISUAL Y COMUNICACIONES VICOMTECH	REC	ES	1
AARHUS UNIVERSITET	HES	DK	1
GMV AEROSPACE AND DEFENCE SA	PRC	ES	1

Source: JRC analysis of Cordis data.

Table 42: Entities participating in at least 2 projects related to "Terrorism financing"

Name of entity	Legal status	Country	Number of projects
TRILATERAL RESEARCH LTD	PRC	UK	3
MINISTERIO DEL INTERIOR	PUB	ES	3
RISSC - CENTRO RICERCHE E STUDI SUSICUREZZA E CRIMINALITA ASSOCIAZIONE	REC	IT	2
AIT AUSTRIAN INSTITUTE OF TECHNOLOGY GMBH	REC	AT	2
MINISTERIO DA JUSTICA	PUB	PT	2

Source: JRC analysis of Cordis data.

Annex 7. Horizon scanning on security: selected items which inspired collective clusters

Misuse of DNA data

A portrait without ever seeing your face: a realistic mugshot using just your DNA

Summary: Scientists trained an algorithm to link facial features to people's genetic code. Using this algorithm the team were able to identify people from their genomes. The study raises privacy concerns for those with their DNA stored in databases. Research volunteers are typically promised anonymity before they give samples. The new research suggests this level of privacy is impossible in the long-run. Using this information, scientists will be able to work back to individuals and figure out their traits, which could lead to business opportunities. "Just like Google and others now sell advertising to you based on what is in your searches and emails, you could get adverts targeted to you based on what's in your genome," Dr Venter added. Tim Hubbard, head of Genome Analysis at Genomics England, the organisation responsible for the 100 000 Genomes Project, told the Times that safeguards were in place to protect the identity of database volunteers. He said that as well as all data being "de-identified", any person, institution or company that attempts to identify people through database DNA is breaking the law. Those doing so could face criminal charges or substantial fines, he said.

Why it could be important? Using this information, scientists will be able to work back to individuals and figure out their traits, which could lead to business opportunities. There are also privacy issues to studying predisposition to addictions.

Date: 5 September 2017; Source URL: <http://www.dailymail.co.uk/sciencetech/article-4853084/Scientists-use-GENES-build-image-face.html>

Building a biobank

Summary: Researchers to create genome sequence database so that treatment can match needs of patients. A pilot project involving three Thai medical research facilities and a China-based genomics company will build a genome-sequence database of Thais in order to better match medical treatment to patient needs. The Thailand Centre of Excellence for Life Sciences (TCELS), Thailand Research Fund (TRF), and Ramathibodi Hospital's Centre for Medical Genomics have together teamed up with Shenzhen-based BGI Genomics, one of the world's genome sequencing centres, to collect the entire genome sequence for Thais. The five-year pilot project will collect the whole 19,000 genome sequencing of 10 000 Thai volunteers. The results of the pilot project would then form the initial data as a national "bio-bank" for Thais is kicked off. The sequencing work will begin at a TCELS lab, before being expanded and moved to Thailand Science Park, which will also serve as the home of the national bio-bank data centre. Sirisak Tapakam, TCELS' deputy director for academic affairs and innovation, said that collected genomic information will help ensure that Thais receive precise medical treatment in future.

Why it could be important? The ultimate goal is also to hope the result of the two genome sequencing projects (the 100 drug-related genes sequences from 1 000 subjects in SEA, and the 19 000 genome sequences from 10 000 Thais) will provide sufficient data to allow government to make decisions about adjusting and improving public health policy and more efficient budget spending.

Date: 25 February 2018; Source URL: http://www.nationmultimedia.com/detail/Startup_and_IT/30339675

How Just 13 DNA Snippets Could Identify You

Summary: Just 13 snippets of DNA may be enough to make conclusions about hundreds of thousands of genetic markers, even those not present in the sample, possibly revealing enough to indicate personal identity information. The new study's results may help foster scientific collaborations and aid researchers working with degraded or incomplete DNA samples, such as those collected from wildlife or archaeological sites, says Noah Rosenberg, a professor of biology at Stanford University and the new paper's senior author. But the ability to infer so much on the basis of so little information raises privacy concerns as well, Rosenberg says. The new findings are based on two sets of genetic data from 872 human genomes. The first comprised just 13 markers that until this year were the basis of the FBI's forensic genetic marker set, the Combined DNA Index System, or CODIS. (The system was recently upgraded to include seven additional markers, bringing the total to 20). The second, much broader dataset included 642 563 genetic markers that did not overlap with the first set. The question was, how well could Rosenberg and his team match a person's record in one dataset to their record in the other? Put differently, how well could they predict the second set of genetic markers based solely on the first, forensic set? Pretty well, actually. Rosenberg and team found there were strong enough patterns in our DNA—or at least in the DNA of the diverse set of people they studied—that they could match upward of 90 percent of the records. If they added in 17 more forensic markers, bringing the total to 30, they could match more than 99 percent of the records in the two datasets—meaning that with the right combination of databases, it may be possible to infer a wealth of genetic information based on a very small set of markers.

Why it could be important? It can help forensics to perform their job in complex cases. There is an ethical issue regarding the privacy of the medical information (genomic information)

Date: 21 May 2017; Source URL: <https://knowridge.com/2017/05/how-just-13-dna-snippets-could-identify-you/>

Threat of gene editing (CRISPR)

CRISPR -- potentially dangerous technology freely available

Summary: Methods of engineering microorganisms' DNA are readily available and getting more powerful. What's more, a new "do it yourself" movement is starting to shift genetic engineering out of large institutions and into DIY labs or people's homes, where it's harder to keep tabs on. Biological expertise can't easily be contained. The challenge is that the same germs, techniques, and skills needed to study disease can also be used as weapons. The result: potentially dangerous technology is freely available. Another security risk is connected to large DNA and biological databases. The US is mounting a million-person precision medicine study that will gather such data, and vast commercial troves exist already. In February, the US declared gene editing, a new way of easily modifying DNA, to be a potential WMD. At the same time, home kits to modify the genes of bacteria using the method, called CRISPR, are on sale online for USD 140.

Why it could be important? While having huge potential positive implications for health, CRISPR also has unpredictable security implications that are yet to be addressed.

Source URL: <https://www.technologyreview.com/s/602643/on-patrol-with-americas-top-bioterror-cop/>

Could CRISPR be used as a biological weapon?

Summary: The gene editing technique CRISPR has been in the limelight after scientists reported they had used it to safely remove disease in human embryos for the first time. This follows a "CRISPR craze" (<http://science.sciencemag.org/content/341/6148/833>) over the last couple of years, with the number of academic publications on the topic growing steadily. There are good reasons for the widespread attention to CRISPR. It allows scientists to "cut and paste" DNA more easily (https://www.labor-spiez.ch/pdf/en/Report_on_the_second_workshop-5-9_September_2016.pdf) than in the past. It is being applied to a number of different peaceful areas, ranging from cancer therapies to the control of disease carrying insects. Some of these applications – such as the engineering of mosquitoes to resist the parasite that causes malaria – effectively involve tinkering with ecosystems. CRISPR has therefore generated a number of ethical and safety concerns. Some also worry that applications being explored by defence organisations (<https://www.darpa.mil/news-events/2016-09-07>) that involve "responsible innovation in gene editing" may send worrying signals to other states. Concerns are also mounting that gene editing could be used in the development of biological weapons. In 2016, Bill Gates remarked that "the next epidemic could originate on the computer screen of a terrorist intent on using genetic engineering to create a synthetic version of the smallpox virus". More recently, in July 2017, John Sotos, of Intel Health & Life Sciences, stated that gene editing research could "open up the potential for bioweapons of unimaginable destructive potential".

Why it could be important? An annual worldwide threat assessment report of the US intelligence community in February 2016 argued that the broad availability and low cost of the basic ingredients of technologies like CRISPR makes it particularly concerning.

Date: 31 August 2017; Source URL: <https://phys.org/news/2017-08-crispr-biological-weapon.html> and <https://www.technologyreview.com/s/600774/top-us-intelligence-official-calls-gene-editing-a-wmd-threat>

Synthetic genome engineering gets infectious

Summary: Since the start of this century, a handful of research groups have pursued the synthesis and large-scale engineering of genomes. Work on synthetic genomes has seen the field scale-up from the full synthesis of the small poliovirus genome (2002), to a complete working synthetic bacterial genome (2010), and more recently to the construction and validation of multiple rewritten eukaryote chromosomes for the model organism *Saccharomyces cerevisiae* (2014, 2017). The costs and time-scales for assembling entire bacterial genomes and eukaryotic chromosomes mean that synthetic genome engineering is not yet a routine approach to manipulating cells for research or biotechnology. However, by stepping down a scale from bacteria to viruses, opportunities quickly arise, even for those viruses with comparatively large genomes, like the double-stranded DNA herpes simplex virus (HSV) type 1 genome, over 150 kb in length. In PNAS, Oldfield et al. engineer the HSV KOS strain genome, leveraging synthetic genomic cloning approaches to rapidly construct HSV variants with combinatorial mutations for functional evaluation. Large-scale genomic engineering has been achieved by a handful of groups taking different approaches, but broadly the strategies employed fall into two categories: multiplexed editing and hierarchical assembly. For editing, new technologies, such as multiplex automated genome engineering-based targeted mutation and the new genome editing tools of CRISPR-Cas9 allow existing genomes to be extensively modified toward a target sequence over several generations within their host cells. This can be an efficient approach if the cell grows fast and is easy to manipulate with molecular biology methods. For the alternative hierarchical assembly strategy, a designed or modified target genome sequence is instead put together gradually from smaller subgenomic fragments that are linked together by various DNA assembly methods. Depending on the size of the genome or chromosome.

Why it could be important? Are we examining the consequences?

Date: 18 October 2017; Source URL: <http://www.pnas.org/content/114/42/11006.short>; doi: 10.1073/pnas.1715365114

Significant quantum and neuromorphic computing advancements

Summary: At the 2018 Consumer Electronics Show in Las Vegas, Intel announced two major milestones: a 49-qubit superconducting quantum test chip and neuromorphic computing. The 49-qubit superconducting quantum test chip code-named "Tangle Lake," will "allow researchers to assess and improve error correction techniques and simulate computational problems." The announcement came just two months after the delivery of a 17-qubit superconducting test chip. The neuromorphic research chip code-named "Loihi" is designed to mimic the way neurons communicate in the brain. Loihi is meant to make machine learning more efficient.

Why it could be important? The neuromorphic chips will help accelerate real-world data processing in evolving real-time environments, e.g. enable smarter security cameras and smart-city infrastructure designed for real-time communication with autonomous vehicles.

Date: 8 January 2018; Source: <https://newsroom.intel.com/news/intel-advances-quantum-neuromorphic-computing-research/>

China's quantum satellite - quantum teleportation and transmitting encryption keys

Summary: In June, Chinese researchers demonstrated that the satellite Micius could send entangled quantum particles to far-flung locations on Earth, their properties remaining intertwined despite being separated by more than 1 200 kilometres. Now researchers have used the satellite to teleport particles' properties and transmit quantum encryption keys. In quantum teleportation, the properties of one particle are transferred to another. The scientists first sent particles of light, or photons, from the ground to the satellite — a distance of up to 1 400 kilometres. When the researchers made particular measurements of other photons on the ground, the spacefaring particles took on the properties of the landlubbers, thanks to quantum entanglement between the earthbound and satellite-based particles – an important ingredient of quantum communication. Quantum key distribution is a method of creating a secret string of random numbers that can be used to encrypt communications. The researchers beamed photons from the satellite to Earth over distances of up to 1 200 kilometres, using the photons' polarization, the orientation of their electromagnetic waves, to transmit a string of random numbers with utmost security. Quantum communication via satellite can reach greater distances than land-based transmission, because in space, particles don't get absorbed by the atmosphere.

Why it could be important? The new results pave the way for a global quantum internet that would provide for ultra-secure communications and allow quantum computers to work together.

Date: 7 July 2017; Source: <https://www.sciencenews.org/article/china-quantum-satellite-adds-two-new-tricks-repertoire>

Control society – surveillance profiling

China piloting nation-wide "social credit rating system"

Summary: China introduces a pilot "social credit system" – an ambitious social-engineering experiment that the Communist Party plans to undertake over the next five years. The system would evaluate the behaviour of individuals and businesses by tapping on vast troves of personal digital data accumulated from its citizens' online activity, such as purchases and other forms of digital presence, as well as data related to food-safety or pollution incidents for firms.

Why it could be important? First attempts to mine personal data and control behaviour based on it.

Date 29 November 2016; Source URL: <http://blogs.wsj.com/chinarealtime/2015/11/06/china-wants-to-tap-big-data-to-build-a-bigger-brother/>

Neo-Lombrosians decide that you are gay by looking at your face

Summary: Lombroso is not dead, in the minds of some... In the study, which involved the examination of more than 35 000 images, it was found that the computer algorithm could correctly distinguish between gay and straight men in 81% of the instances. For women, this number was 74%. When the software reviewed five images per person, this accuracy rocketed up to 91%. The researchers, Dr. Kosinski and Mr. Wang, have also offered an explanation for this outcome. According to them, as a fetus grows in mother's womb, it's exposed to different hormones—including testosterone—that play a part in the development of facial structures. The AI model is able to pick the subtle signals of a person's sexuality from a man's nose, eyes, eyebrows, cheeks, hairline, and chin. For women, the most important parts are nose, mouth corners, hair, and neckline.

Why is it important? In contrast to the algorithms, the human judges performed much poorly. They accurately identified the sexual orientation correctly 54% of the time for women and 61% for men.

Date: 8 September 2017; Source: <https://fossbytes.com/ai-tells-gay-or-straight-from-pictures/>

Would YOU let your boss implant you with a microchip?

Summary: NewFusion is offering to implant the identification chips in employees' hands. Chips contain personal information and provide access to the company systems 10 000 people worldwide are believed to already have microchip implants.

Why it could be important? Controversial devices raise questions about personal security and safety.

Date: 8 February 2017; Source: <http://www.dailymail.co.uk/sciencetech/article-4203148/Company-offers-RFID-microchip-implants-replace-ID-cards.html>

Autonomous weapons

Open letter to stop lethal autonomous weapons becoming the third revolution in warfare

Summary: Lethal autonomous weapons threaten to become the third revolution in warfare. Once developed, they will permit armed conflict to be fought at a scale greater than ever, and at timescales faster than humans can comprehend. These can be weapons of terror, weapons that despots and terrorists use against innocent populations, and weapons hacked to behave in undesirable ways. We do not have long to act. Once this Pandora's box is opened, it will be hard to close. We therefore implore the High Contracting Parties to find a way to protect us all from these dangers. This is the call of AN OPEN LETTER TO THE UNITED NATIONS CONVENTION ON CERTAIN CONVENTIONAL WEAPONS signed by an excellence group of developers and entrepreneurs in AI and robotics.

Why is it important? "As companies building the technologies in Artificial Intelligence and Robotics that may be repurposed to develop autonomous weapons, we feel especially responsible in raising this alarm. We warmly welcome the decision of the UN's Conference of the Convention on Certain Conventional Weapons (CCW) to establish a Group of Governmental Experts (GGE) on Lethal Autonomous Weapon Systems. Many of our researchers and engineers are eager to offer technical advice to your deliberations. Nevertheless, as a Guardian article explains, We can't ban killer robots – it's already too late".

Date: 20 August 2017; Sources: AN OPEN LETTER TO THE UNITED NATIONS CONVENTION ON CERTAIN CONVENTIONAL WEAPONS <https://futureoflife.org/autonomous-weapons-open-letter-2017/>; We can't ban killer robots – it's already too late: <https://www.theguardian.com/commentisfree/2017/aug/22/killer-robots-international-arms-traders>

The Malicious Use of Artificial Intelligence

Summary: A 100-page report released today (February 21, 2018) is sounding the alarm about the risks of malicious use of artificial intelligence by "rogue states, criminals, terrorists". "As AI capabilities become more powerful and widespread, we expect the growing use of AI systems to lead to the following changes in the landscape of threats: (1) Expansion of existing threats. The costs of attacks may be lowered by the scalable use of AI systems to complete tasks that would ordinarily require human labour, intelligence and expertise. A natural effect would be to expand the set of actors who can carry out particular attacks, the rate at which they can carry out these attacks, and the set of potential targets. (2) Introduction of new threats. New attacks may arise through the use of AI systems to complete tasks that would be otherwise impractical for humans. In addition, malicious actors may exploit the vulnerabilities of AI systems deployed by defenders. (3) Change to the typical character of threats. We believe there is reason to expect attacks enabled by the growing use of AI to be especially effective, finely targeted, difficult to attribute, and likely to exploit vulnerabilities in AI systems". (4) Why is it important? This report surveys the landscape of potential security threats from malicious uses of artificial intelligence technologies, and proposes ways to better forecast, prevent, and mitigate these threats. The focus is "on what sorts of attacks we are likely to see soon if adequate defences are not developed."

Date: 21 February 2018; Source: <https://maliciousaireport.com/> ;

See also: <https://connected.cnect.cec.eu.int/community/jrc/directorate-e/e7/blog/2017/11/30/security-and-defense-artificial-intelligence-and-potentially-catastrophic-consequences-of-allowing-lethal-autonomous-weapons-to-be-developed>; Fake video on mini-drone killers for real questions: <http://www.lemonde.fr/videos/#v50lf0>; - Future of Life Institute: <https://futureoflife.org/>; Artificial Intelligence and Safety Research: <https://futureoflife.org/ai-safety-research/>; Call for autonomous weapons ban at the UN: <http://autonomousweapons.org/>

Brain manipulation

Brainwave technologies to read thoughts

Brainwave technologies will be used in various products in the years to come, they have already started: Actually a number of companies already sell basic brain wave reading devices; some companies offer headsets that allow you to play a video game on your iPhone using only thoughts. NeuroSky's MindWave (<http://neurosky.com/>) can attach to Google Glass and allow you to take a picture and post it to Facebook and Twitter just by thinking about it. Even the army has (not very well) flown a helicopter using only thoughts and a brain wave headset.

Why is important? Human computer interaction with a brain reader allows gathering conscious and unconscious brain activities. This could be a way for better understanding the intentions and wishes of people but comes with a dystopian scenario of Big Brother surveillance. Practical use for touchless human machine interaction (e.g. brain computer interface) is another field of application.

Date: July 2010, April 2017; Source: https://www.ted.com/talks/tan_le_a_headset_that_reads_your_brainwaves and <https://techcrunch.com/2017/04/19/facebook-brain-interface/>

How electrical brain stimulation can change the way we think

Summary: US military researchers have had great success using “transcranial direct current stimulation” (tDCS) — in which they hook you up to what’s essentially a 9-volt battery and let the current flow through your brain. After a few years of lab testing, they have found that tDCS can more than double the rate at which people learn a wide range of tasks, such as object recognition, math skills, and marksmanship. After trying it myself, I have different questions. To make you understand, I am going to tell you how it felt. The experience wasn’t simply about the easy pleasure of undeserved expertise. For me, it was a near-spiritual experience. When a nice neuroscientist named Michael Weisend put the electrodes on me, what defined the experience was not feeling smarter or learning faster: The thing that made the earth drop out from under my feet was that for the first time in my life, everything in my head finally shut up. There was suddenly this incredible silence in my head; I have experienced something close to it during two-hour Iyengar yoga classes, or at the end of a 10k, but the fragile peace in my head would be shattered almost the second I set foot outside the calm of the studio.

Why it could be important? And then, finally, the main question: What role do doubt and fear play in our lives if their eradication actually causes so many improvements? Do we make more ethical decisions when we listen to our inner voices of self-doubt or when we’re freed from them? If we all wore these caps, would the world be a better place?

Date: 30 March 2012; Source: <http://theweek.com/articles/476866/how-electrical-brain-stimulation-change-way-think>

Nightmare weekend? Don’t worry, removing bad memories is a step closer

Summary: New research shows that weakening the connections between specific groups of brain cells can prevent the recall of fear memories in mice. The study, published earlier this week in the journal *Neuron*, has led some – including the study authors themselves – to speculate that this will eventually lead to treatments for conditions such as post-traumatic stress disorder and, inevitably, to news stories mentioning the 2004 film *Eternal Sunshine of the Spotless Mind*, in which an estranged couple undergo a procedure to erase memories of each other from their brains. Woong Bin and Jun-Hyeong Cho of the University of California, Riverside used a combination of sophisticated techniques to identify those brain cells in mice that encode a specific type of fearful memory, and then to suppress them, so that the memory could not subsequently be “reactivated”. Contrary to some of the news stories, however, this is not “a new approach to wiping memories from the brain”. Over the past five years, there has been a whole series of studies using optogenetics to manipulate memories in various ways, most notably from Susumu Tonegawa’s lab at the Massachusetts Institute of Technology (<https://tonegawalab.mit.edu/>). The novelty of this new study is the identification of the neuronal circuitry that encodes this particular type of fear memory – it has determined exactly which cells in the mouse brain do so and, equally importantly, the precise pattern of the connections they form with neurons in other parts of the brain. This trial involves injecting a virus carrying the Channelrhodopsin gene into patients’ eyes, in the hope that it will be taken up by cells in the retina, so that natural light entering the eyes will stimulate them to send signals along the optic nerve to the brain. The effectiveness of such a treatment remains to be seen, and optogenetic treatments for manipulating memories in the human brain face far bigger challenges. (<https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3868662/>).

Why it could be important? Research like this should continue to advance our understanding of how the brain works, by revealing more of the finer details about how its cells function together to encode, store and retrieve different kinds of memories.

Date: 21 August 2017; Source: <https://www.theguardian.com/commentisfree/2017/aug/21/nightmare-weekend-remove-bad-memories-step-closer>

Mind-reading algorithm uses EEG data to reconstruct images based on what we perceive

Summary: A new technique developed by neuroscientists at the University of Toronto Scarborough can, for the first time, reconstruct images of what people perceive based on their brain activity gathered by EEG. The technique developed by Dan Nemrodov, a postdoctoral fellow in Assistant Professor Adrian Nestor’s lab at U of T Scarborough, is able to digitally reconstruct images seen by test subjects based on electroencephalography (EEG) data. “When we see something, our brain creates a mental percept, which is essentially a mental impression of that thing. We were able to capture this percept using EEG to get a direct illustration of what’s happening in the brain during this process,” says Nemrodov. For the study, test subjects hooked up to EEG equipment were shown images of faces. Their brain activity was recorded and then used to digitally recreate the image in the subject’s mind using a technique based on machine learning algorithms. It is not the first time researchers have been able to reconstruct images based on visual stimuli using neuroimaging techniques. The current method was pioneered by Nestor who successfully reconstructed facial images from functional magnetic resonance imaging (fMRI) data in the past, but this is the first time EEG has been used.

Why it could be important? The fact we can reconstruct what someone experiences visually based on their brain activity opens up a lot of possibilities. It unveils the subjective content of our mind and it provides a way to access, explore and share the content of our perception, memory and imagination.

Date: 22 February 2018; Source: https://www.eurekalert.org/pub_releases/2018-02/uot-mau022218.php

Misuse of robotisation

The Day Humans Taught Robots to Fight Back

Summary: An amazing video of a robot dog fighting off a human as it tries to open a door is not only creepy, but it also has raised the question: Why are we teaching a robot to fight back against humans? The “dog” in question is the SpotMini, a 66-lb. (30 kilograms) robot designed to fit comfortably in a home or an office. In the video, the dog is shown attempting to open a door—when a human comes with a hockey stick and shoves the robot’s grasping arm away from the door knob. The robot manages to open the door anyway, and even continues standing when a human tries to pull “him” away from the door using a huge leash. It turns out, any successful robot assistant for the home needs to be good at dealing with “disturbances”, according to the company — and that may sometimes include pesky humans.

Why it could be important? Needs for regulation

Date: 22 February 2018; Source: <https://www.livescience.com/61840-robot-dog-fights-off-human.html>

Airbus’ Self-Flying Taxi Drone Takes First Flight

Summary: Airbus first announced its plans to create a self-flying taxi service in 2016. On Jan. 31, after two years of planning and building, it proved it isn’t just a pipedream — the Vahana successfully completed its first flight test. Only one person can fit in the electric VTOL (vertical takeoff and landing) drone. It measures about 20 feet wide, 19 feet long, 9 feet high and weighs more than 1 600 pounds. Discover has reported that Uber is looking to add self-flying aircraft like these to their services.

Why is it important? If successful, it would democratize personal flight giving a strong boost to technologies such as electric propulsion, energy storage, and machine vision.

Date: 2 February 2018; Source: <http://blogs.discovermagazine.com/drone360/2018/02/02/airbus-drone-flying/>

Overreliance on AI

Nudged by machines

Summary: Digital assistants have much to offer, but the next technological frontier may not be entirely rosy. As our digital butler increasingly controls our mundane tasks, it will be harder to turn off. It will be tempting to increasingly rely on the butler for the news we receive, the shows we watch, and the things we buy and even say. We may feel that we roam the fields of free ideas. And yet, we are increasingly ushered by the super-platform’s digitalized hand, not recognizing its toll on our well-being.

Why it could be important? Many of our decisions will be done by the digital assistants in the future.

Date: 8 December 2016; Source: <https://www.wired.com/2016/11/subtle-ways-digital-assistant-might-manipulate/>

Machine bias: urgent need to understand algorithmic bias

Summary: Algorithmic bias is shaping up to be a major societal issue at a critical moment in the evolution of machine learning and Artificial Intelligence. Algorithms that may conceal hidden biases are already routinely used to make vital financial and legal decisions. Society will start to trust the mathematical (data-driven) models only if there are agreed procedures for the identification, monitoring and correction of the algorithmic biases.

Why is this important? Policy making: regulation of the algorithms use; Data-driven modelling: accept responsibility.

Date: July 2017 Source: https://www.youtube.com/watch?v=fMym_BKWQzk&t=6s and <https://weaponsofmathdestructionbook.com/>

Subversion of government – new governance

Backfeed: an operating system for decentralised organisations

Summary: A new operating system for organisations, called Backfeed, aims to enable “large-scale, free and systematic cooperation between thousands of people without the coordination of any central authority”. It is founded upon a peer-to-peer evaluation system, based on tokens that are recorded on blockchains. The tokens represent the perceived value of individual contributions to a community and enable the organisation to compensate accordingly.

Why is it important? This is part of a growing wave of ‘platform co-operativism’, in which businesses are owned and controlled by the services users themselves. It is evidence of the Sharing Economy coming to maturity, and the regeneration of co-operatives. It may change the way people live and travel, and the way urbanisation will develop, countering the current trend to develop mega-cities.

Date: 8 November 2016; Sources: <https://www.forumforthefuture.org/blog/signal-change-backfeed-operating-system-decentralised-organisations> and <http://backfeed.cc/explore-in-depth>

Individualistic practices and values increasing around the world

Summary: Individualism is thought to be on the rise in Western countries, but new research suggests that increasing individualism may actually be a global phenomenon. The findings, published in *Psychological Science*, a journal of the Association for Psychological Science, show that increasing socioeconomic development is an especially strong predictor of increasing individualistic practices and values in a country over time. "Much of the research on the manifestation of rising individualism – showing, for example, increasing narcissism and higher divorce rates – has focused on the United States. Our findings show that this pattern also applies to other countries that are not Western or industrialized," says psychology researcher Henri C. Santos of the University of Waterloo. "Although there are still cross-national differences in individualism-collectivism, the data indicate that, overall, most countries are moving towards greater individualism". Overall, the results showed a clear pattern: Both individualistic practices and values increased across the globe over time. Specifically, statistical models indicated that individualism has increased by about 12% worldwide since 1960.

Why it could be important? Santos and Grossmann are hoping to continue this line of research, studying other predictors of cultural change, including migration and shifts in ethnic diversity, and also the potential consequences that rising individualism may have on a global scale. "I hope that these findings encourage psychologists in a variety of countries to take a more in-depth look at the rise of individualism within their respective countries," says Santos.

Date: 18 July 2017; Source: https://www.eurekalert.org/pub_releases/2017-07/afps-ipa071717.php and <http://journals.sagepub.com/doi/full/10.1177/0956797617700622>

Asgardia: first nation state in space

Summary: A team of scientists and legal experts is welcoming people to join the first space nation, Asgardia (<https://asgardia.space/en/>), coined as "a global, unifying and humanitarian project". According to Head of Nation Dr. Igor Ashurbeyli (<https://asgardia.space/en/page/concept>), the aim is for Asgardia to become a full-fledged independent nation, and a member of the United Nations. As a conflict-free no-man's land, Asgardia will mirror humanity in space, minus the divisiveness of states, religions and nations. With false divides collapsed, everyone will be equal regardless of the prosperity of the country they happened to be born in.

Why it could be important? With today's commercialisation of space through activities such as asteroid mining, we risk seeing companies and nations at the forefront setting anti-competitive rules and monopolies. On the legal front, Asgardia seeks to create a 'Universal space law' and 'astropolitics' to protect the interests of developing nations as well as open up access to space technology. Using protective shields Asgardia also wants to defend Earth against cosmic threats such as asteroids and space junk.

Date: 24 Mar 2017; Source: <https://www.theguardian.com/science/2016/oct/12/will-you-become-a-citizen-of-asgardia-the-first-nation-state-in-space>

Media changing the society

Post-truth and self-administered justice

Summary: Pizzagate, the conspiracy theory that claims (with no evidence) that high-ranking Democratic officials and allies operate an international pedophilia ring centered around Washington, DC's Comet Pizza (http://dcist.com/2016/12/what_on_earth_is_pizzagate_why_did.php), made a cameo in New York City this month when employees of Roberta's received threatening phone calls related to the internet fixation. Pizzagate hopped off the virtual pages of some of the internet's most notorious sewers and into real life this weekend, when an armed man walked into Comet Pizza and fired a gun, while claiming he was there (http://dcist.com/2016/12/alleged_comet_ping_pong_gunman_says.php) to self-investigate the claims of the conspiracy theory.

Why it could be important? Interconnectedness made conspiracy theories more potent, but with the weakening of perception of government, people are more willing to act on them.

Date: 8 December 2016; Source: http://gothamist.com/2016/12/07/robertas_gets_threatening_pizzagate.php

Both the aggressor and the victim: alarming number of teens cyberbully themselves

Summary: Adolescents harming themselves with cuts, scratches or burns has gained a lot of attention over the years not just because of the physical damage and internal turmoil, but also because it has been linked to suicide. More recently, a new form of self-harm in youth has emerged and is cause for concern, warns a researcher and bullying expert from Florida Atlantic University. The behaviour: "digital self-harm," "self-trolling," or "self-cyberbullying," where adolescents post, send or share mean things about themselves anonymously online. The concern: it is happening at alarming rates and could be a cry for help. A new FAU study is the first to examine the extent of this behaviour and is the most comprehensive investigation of this understudied problem. "The idea that someone would cyberbully themselves first gained public attention with the tragic suicide of 14-year-old Hannah Smith in 2013 after she anonymously sent herself hurtful messages on a social media platform just weeks before she took her own life," said Sameer Hinduja, Ph.D., study author, a professor in FAU's School of Criminology and Criminal Justice in the College for Design and Social Inquiry, and co-director of the Cyberbullying Research Center. "We knew we had to study this empirically, and I was stunned to

discover that about 1 in 20 middle- and high-school-age students have bullied themselves online. This finding was totally unexpected, even though I've been studying cyberbullying for almost 15 years".

Why it could be important? "Prior research has shown that self-harm and depression are linked to increased risk for suicide and so, like physical self-harm and depression, we need to closely look at the possibility that digital self-harm behaviours might precede suicide attempts," said Hinduja. "We need to refrain from demonizing those who bully, and come to terms with the troubling fact that in certain cases the aggressor and target may be one and the same. What is more, their self-cyberbullying behaviour may indicate a deep need for social and clinical support."

Date: 30 October 2017; Source: https://www.eurekalert.org/pub_releases/2017-10/fau-bta103017.php

Why you should be sceptical that any video is real

Summary: Researchers have shown how a video of a person talking can be altered in real time to change what a speaker appears to be saying. In a new video, the scientists show how they edited YouTube clips to change mouth movements. The system uses a webcam to track one person's facial expressions, and then applies them to the face of the person in the target video. The software creates a 3D representation of a subject's face, which can then be swapped with the 3D representation of another face. The process works even if one subject has facial hair or a different skin tone. But it won't work if a person's long hair blocks his or her mouth.

Why it could be important? Matthias Niessner, a Stanford University professor who contributed to the collaboration between the University of Erlangen-Nuremberg and the Max Planck Institute, warned that because of such technology we should be more careful about believing what we see in videos.

Date: March 2016; Source: <https://www.washingtonpost.com/news/innovations/wp/2016/03/23/why-you-should-be-skeptical-that-any-video-is-real/> <http://niessnerlab.org/projects/thies2016face.html>

High-tech crime

New governance forms of organised crime

Summary: An increasing number of individual criminal entrepreneurs offer Crime-as-a-Service (CaaS). The online trade in illicit goods and services enables individual criminals to operate their own criminal business without the need for the infrastructures maintained by 'traditional' organised crime groups (OCGs). OCGs exploit various legal business structures and professional experts to maintain a facade of legitimacy, obscure criminal activities and profits, and to perpetrate lucrative and complex crimes. Legal business structures allow OCGs to operate in the legal economy and enable them to merge legal and illegal profits.

Why it could be important? Organised crime is not necessarily hierarchical structure.

Source: EUROPEAN UNION SERIOUS AND ORGANISED CRIME THREAT ASSESSMENT Crime in the age of technology "SOCTA2017", Europol <https://www.europol.europa.eu/activities-services/main-reports/european-union-serious-and-organised-crime-threat-assessment-2017>

Audio speakers hacked and transformed in spy bugs

Summary: Research by MWR InfoSecurity (<https://labs.mwrinfosecurity.com/blog/alexa-are-you-listening>) found it is possible to turn an Amazon Echo into a covert listening device without affecting its overall functionality. One big limiting factor: the process does involve the attacker being able to gain access to the physical unit, but it is possible to tamper with the Echo without leaving any evidence.

Why is it important? Hacking and spying will grow and merge, with hackers more and more connected to commercial and international spying cybersecurity issues will become more and more relevant. Customers need to be informed of side effects of technology.

Date: 1 August 2017; Sources: <http://www.zdnet.com/article/this-amazon-echo-hack-can-make-your-speaker-spy-on-you-say-security-researchers/> <https://labs.mwrinfosecurity.com/blog/alexa-are-you-listening>

Crowdsourcing police work

Summary: Police departments are often overloaded with cases, making it difficult to devote 40-plus hours a week to a 20-year-old case. That's where podcasters can be a big help. The best recent example of that is the well-known podcast Serial (<https://serialpodcast.org/>). The podcast, which won a Peabody Award, also helped lead to a new trial (<http://www.cnn.com/2016/08/02/us/adnan-syed-serial-new-trial-appeal/>) for Syed, based largely on the very inconsistencies Koenig pointed out in her series. The number of true crime podcasts almost immediately began multiplying, capitalizing on the many true crime fans who were seeking similar podcasts as Serial came to an end. Serial inspired an offshoot podcast called Undisclosed (<http://undisclosed-podcast.com/>), which took a more in-depth look into Syed's case. In the process, the show's co-host discovered the cell phone tower evidence that was eventually used to overturn the original conviction. "As a community in general, we are very cognizant of the impact podcasts like Serial and Undisclosed have had in the legal community," Lopez says. "People thought Adnan's conviction being overturned was impossible, and Undisclosed proved that it wasn't. That is huge."

Why it could be important? A combination of new media and citizen engagement can be used in less obvious domains like security.

Date: 14 February 2017; Source: <https://psmag.com/in-an-internet-era-can-armchair-detectives-actually-solve-a-case-be0a90aa9db5#.npr0fmugh>

Blurring between security and defence

Smartphone App detects military bases

Summary: Sensitive information about the location and staffing of military bases and spy outposts around the world has been revealed by a fitness tracking company. The details were released by Strava (<https://www.strava.com/>) in a data visualisation map that shows all the activity tracked by users of its app, which allows people to record their exercise and share it with others. The map, released in November 2017, shows every single activity ever uploaded to Strava – more than 3 trillion individual GPS data points, according to the company. The app can be used on various devices including smartphones and fitness trackers like Fitbit to see popular running routes in major cities, or spot individuals in more remote areas who have unusual exercise patterns. However, over the weekend military analysts noticed that the map is also detailed enough that it potentially gives away extremely sensitive information about a subset of Strava users: military personnel on active service. Following the revelations, militaries around the world are contemplating bans on fitness trackers to prevent future breaches. As well as the location of military bases, the identities of individual service members can also be uncovered, if they are using the service with the default privacy settings.

Why it could be important? The US Marines have had clear policies on the use of “personal wearable fitness devices” on base since 2016. Such devices are prohibited “if they contain cellular or wifi, photographic, video capture/recording, microphone, or audio recording capabilities.” The policy notes that “merely disabling the cellular, camera, or video capability is not sufficient”. But it does allow such devices if they don’t contain those features, and explicitly mentions that devices with bluetooth connectivity and a GPS tracking function may be used on base, and it contains no specific ban on uploading that information. Those features are what allow apps like Strava to create personalised maps of historic activity.

Date: 28 January 2018; Source: <https://www.theguardian.com/world/2018/jan/28/fitness-tracking-app-gives-away-location-of-secret-us-army-bases>

World’s 1st Laser Weapon Is Ready to Blast Rogue Drones

Summary: The world’s first laser weapon — one that can “kill” threatening, airborne drones — is ready for action, according to news sources. The laser, known as the Laser Weapons System (LaWS), may seem as though it were pulled straight from a James Bond movie, but it is entirely functional and can shoot with stunning accuracy, the US Navy told CNN. The LaWS is currently deployed aboard the USS Ponce, an amphibious transport ship, in the Persian Gulf. The LaWS laser beam is completely silent and invisible. It is also fast: The laser travels at the speed of light (186 000 miles per second, or about 300 000 kilometres per second), meaning it is about 50 000 times the speed of an incoming intercontinental ballistic missile, such as the one North Korea is testing, the Navy told CNN. The \$40 million system requires a team of three to operate it and a small generator to power its electricity supply, according to the Navy. However, each blast is relatively cheap.

Why it could be important? Under Geneva Convention rules, armed forces are not allowed to use laser weapons directly against people, reported Optics.org, a site that tracks the photonics industry. The US will abide by that protocol, Rear Adm. Matthew Klunder, chief of naval research, said in 2014 at a news conference in Washington, D.C., according to Optics.org. The US Navy is already developing second-generation systems that might be able to target threats other than drones and water vessels.

Date: 18 July 2017; Source: <https://www.livescience.com/59846-navy-laser-weapon-blasts-drones.html>

Concrete as top weapon on the battlefield

Summary: Concrete is as symbolic to their deployments as the weapons they carried. No other weapon or technology has done more to contribute to achieving strategic goals (<http://www.cbsnews.com/news/full-transcript-of-bushs-iraq-speech/>) of providing security, protecting populations, establishing stability, and eliminating terrorist threats. This was most evident in the complex urban terrain of Baghdad, Iraq. Increasing urbanization and its consequent influence on global patterns of conflict mean that the US military is almost certain to be fighting in cities again in our future wars. Military planners would be derelict in their duty if they allowed the hard-won lessons about concrete learned on Baghdad’s streets to be forgotten.

Why could it be important? Should the military incorporate concrete into its plans for contingencies in urban terrain? Should it equip Army combat formations with better cranes among its organic equipment? Should the Army pre-position concrete? Should research and development be conducted on advanced hydraulic systems or technology that lifts six-ton barriers so that a soldier can push them into place by hand? These are questions that military planners should be asking. Concrete might not be sexy, but it is the most effective weapon on the modern battlefield.

Date: 22 December 2016 Source: <http://mwi.usma.edu/effective-weapon-modern-battlefield-concrete/>

Decrease of privacy

Human rights and automated border controls

Summary: In 2013, the European Union proposed expanding and harmonizing automated border crossings across the region. This Smart Borders initiative could soon be approved. The automated gates (e-gates) in place in many EU airports are the first phase. The European Agency for the Operational Management of Large-scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA) is testing how to link them to databases and processes region-wide. Entries and exits will be stored in a database, replacing passport stamps. This information will be made available to border-control and immigration authorities, and will be linked to fingerprint records and watch lists held by police, customs and immigration agencies.

Why it could be important? A piece on technological developments in creation of 'big data borders' and how they endanger human rights (privacy, data security, non-discrimination, right to avoid suspicion) and produce inequalities. Of relevance to transport and security policies, justice and fundamental rights. When our personal data are collected and shared before we board an aeroplane, a border ceases to be a line that separates countries or administrative areas. It becomes a process of monitoring, control and automated decisions. The physical border is increasingly irrelevant because our rights, privileges, relations, characteristics and risk levels are checked all the time.

Date: 9 March 2017; Source: <http://www.nature.com/news/protect-rights-at-automated-borders-1.21543>

Digital Health/Public Health Informatics

Summary: The digital revolution is ongoing and nearly everything is affected by it. The opportunities for interdisciplinary digital health research bringing together computer science to improve public health, global health and wellbeing of individuals, populations and ecosystems globally are numerous.

Why it could be important? The questions that need to be raised however are concerning the risks of these trends. Who owns the data? How is the security organized/regulated? Avoidance of digital dictatorship should be prioritized.

Source: <http://www.acm-digitalhealth.org/>

New law enforcement techniques

Big brother: sunglasses equipped with facial recognition technology

Summary: Police in China have begun using sunglasses equipped with facial recognition technology to identify suspected criminals. The glasses are connected to an internal database of suspects, meaning officers can quickly scan crowds while looking for fugitives. China is a world leader in facial recognition technology and regularly reminds its citizens that such equipment will make it almost impossible to evade the authorities. The country has been building what it calls "the world's biggest camera surveillance network".

Why it is important? Fight criminality but also track political dissidents or profile ethnic minorities.

Date: 7 February 2018; Source: <http://www.bbc.com/news/world-asia-china-42973456>

The next generation of cameras might see behind walls

Summary: The latest camera research is shifting away from increasing the number of mega-pixels towards fusing camera data with computational processing. The single pixel camera captures information from many light sources with a single pixel – for example a simple data projector that illuminates the scene one spot at a time or with a series of different patterns. This form of imaging would allow you to create cameras that work at wavelengths of light beyond the visible spectrum, where good detectors cannot be made into cameras. It is even possible to capture images from light particles that have never even interacted with the object we want to photograph, taking advantage of the idea of "quantum entanglement". This has intriguing possibilities for looking at objects whose properties might change when lit up, such as the eye. For example, does a retina look the same when in darkness as in light? The Lytro camera that collects information about light intensity and direction on the same sensor, to produce images that can be refocused after the image has been taken. The Light L16 camera, with more than ten different sensors, combines all the data to provide a 50 Mb, re-focusable and re-zoomable, professional-quality image. Researchers are also working hard on the problem of seeing through fog, seeing behind walls (<https://www.nature.com/articles/ncomms1747>), and even imaging deep inside the human body and brain (<https://www.nature.com/articles/nphoton.2014.107>). All of these techniques rely on combining images with models that explain how light travels through or around different substances. Another interesting approach that is gaining ground relies on artificial intelligence to "learn" to recognise objects from the data (<https://www.osapublishing.org/optica/abstract.cfm?uri=optica-4-9-1117>). Single photon and quantum imaging technologies are also maturing to the point that they can take pictures with incredibly low light levels and videos with incredibly fast speeds reaching a trillion frames per second.

Why it could be important? One day we may not even need cameras in the conventional sense any more. Instead we will use light detectors that only a few years ago we would never have considered any use for imaging. And they will be able to do incredible things, like see through fog, inside the human body and even behind walls.

Date: 22 January 2018; Source: <https://theconversation.com/the-next-generation-of-cameras-might-see-behind-walls-90258>

Cellphone tracking for outbreaks

Summary: The idea is to find out very quickly the origin of a new infection (accidental or criminal). Usually when there is a new epidemic people are doing an outbreak investigation through a survey among the affected people and relatives in order to discover what they can have had in common (food, water, specific common places, etc.). In this paper the idea is to use the history of recent locations of affected people through their cell phones (ethically not possible right now, but this is an exercise done in Israel). Then you compare the tracking of people obtained through their cell phone and try to find where they have been together...

Why is it important? Apparently it reduces the time from 24 hours (usually required when using surveys), to 4 hours and it could even be quicker if the tracking was more accurate (here the information is obtained through cell phone companies and signal from antenna). Of course it can only be done once people are showing symptoms... so the attack/event may have occurred several days before depending on the incubation period. But once it starts then you can define the exact location and also people who may have also been exposed.

Date: February 2018; Source: <https://www.liebertpub.com/doi/full/10.1089/hs.2017.0012>

Robotisation – impact on society

Post-work: the radical idea of a world without jobs

Summary: As a source of subsistence, let alone prosperity, work is now insufficient for whole social classes. In the UK, almost two-thirds of those in poverty – around 8 million people – are in working households. In 2017, half of recent UK graduates were officially classified as “working in a non-graduate role”. In the US, “belief in work is crumbling among people in their 20s and 30s”, says Benjamin Hunnicutt, a leading historian of work. “They are not looking to their job for satisfaction or social advancement”. Hester would like the post-work movement to think more radically about the nuclear home and family. Both have been so shaped by work, she argues, that a post-work society will redraw them. The disappearance of the paid job could finally bring about one of the oldest goals of feminism: that housework and raising children are no longer accorded a lower status. With people having more time, and probably less money, private life could also become more communal, she suggests, with families sharing kitchens, domestic appliances, and larger facilities.

Why is it important? “A post-work society is meant to resolve conflicts between different economic interest groups – that’s part of its appeal,” he told me. Tired of the never-ending task of making work better, some socialists have latched on to post-work, he argues, in the hope that exploitation can finally be ended by getting rid of work altogether.

Date: 19 January 2018 Source: <https://www.theguardian.com/news/2018/jan/19/post-work-the-radical-idea-of-a-world-without-jobs>

Increasing support for a universal basic income

Summary: Support for a Basic Income Guarantee (BI) is increasing around the world. It is largely accepted that a BI could unleash creativity and encourage new work forms that could reduce unemployment, underemployment, encourage entrepreneurship, encourage consumption at least at replacement levels, avoid eventual social unrest and reduce work-related health risks. Some 68% of EU-28 supports the principle of a BI. Previous pilot programs showed clear benefits and more pilots are being currently conducted and planned. The idea is also supported by tech moguls, some already funding pilot projects. In New Zealand, which will hold national elections this month, a BI is being actively debated. The new TOP party has it as one of their main platform items (No 7) and the Labour Party is also discussing it and considering a “local version”.

Why is it important? Basic income would be a major departure from current active social and employment policy. Would it lend itself to integration, could it be a common policy?

Date: July-August 2017; Sources: <https://futurism.com/richard-branson-just-endorsed-basic-income-here-are-10-other-tech-moguls-who-support-the-radical-idea/> <http://www.oecd.org/employment/emp/Basic-Income-Policy-Option-2017.pdf>

Mining Minerals in space: a reality in 20 years?

Summary: Scientists believe there is an abundance of valuable resources in asteroids and comets that circle around the Sun at about the same speed and distance as the Earth orbits the Sun. An Australian study investigated the potential economic benefits of an off-Earth operation for asteroids. This study examined the metallic asteroid 1986 DA, which is 2.3 km diameter and contains 88% iron, 10% nickel and 0.5% cobalt. Asteroid 1986DA is also estimated to contain more than 10,000 tonnes of gold and 100 000 tonnes of platinum. It is located approximately 75 million km from the Earth – a similar distance between the Earth and Mars – at the closest point of its orbit. The study concluded that extracting minerals from this asteroid and bringing back to Earth is not economically viable, but if the asteroid is halfway closer to the Earth then the operation starts becoming viable. Considering that there are about two million Near Earth Asteroids, it's not hard to see that commercial launch systems and advanced robotics technologies will soon make space-based mining financially viable. Previous research has found that asteroids have several commodities of interest: water and volatiles, precious metals, rare earth minerals, refractory materials, iron and nickel. Comets, on the other hand, have been viewed by the naked eye from the Earth and contain a mixture of gas, dust and water vapour. However, water must be considered the most important commodity in the development of a space economy. Hydrolysis of water produces hydrogen and oxygen, which can be used as a rocket fuel to resupply satellites and spacecraft. Hence there is a common belief that water will be the currency of space. The Moon will most probably be the first off-Earth body that humans colonise. The colonisation purpose most likely will be for tourism or as a staging post for missions to Mars or beyond. According to most researchers and futurists, the Moon regolith would be an ideal material that can be used to construct facilities required by humans. Furthermore, yttrium, lanthanum, and samarium are increasingly critical in the manufacturing of high-tech products such as tablet computers, electric vehicles and wind turbines, and helium-3 is a non-radioactive nuclear fusion fuel that is considered the safest energy source of the future. All of these are abundant on the Moon. Many researchers agree that Mars is the most logical destination for the next manned visit to interplanetary space.

Why is it important? "Off-Earth mining has the potential to trigger great expansion in the global economy (...). We also need to make sure we have trained manpower to take advantage of this great adventure" says Michael Dello-Iacovo, a former geophysicist and researcher in the area.

References: Text mainly based on: Mining Minerals in Space. *Australian Science*, October 2016.

Mars Colony in situ resource utilization: An integrated architecture and economics model. Robert Shishko, Rene Fradet, Sydney Do, Serkan Saydam, Carlos Tapia-Cortez, Andrew G. Dempster, Jeff Coulton. *Acta Astronautica*, 138 (2017) 53–67.

Finnish Cities To Explore Small Modular Reactors For District Heating

Summary: The Finnish cities of Helsinki, Espoo and Kirkkonummi have begun studies to find out if it would be feasible to replace coal and natural gas in district heating with small modular nuclear reactors (SMRs), the environmental group Ecomodernist Society of Finland said. The society said a feasibility study will be carried out into the potential for SMRs to replace fossil fuel-burning in cities around the Helsinki metropolitan area. Several advanced SMRs are in development and coming to market by 2030 that could meet the specifications, the society said.

Why it could be important? Most of the district heating in Finland is produced by burning coal, natural gas, wood fuels and peat. While many Finnish cities have progressive climate policies and goals, they have struggled to decarbonise heating and liquid fuels, the society said. Rauli Partanen, vice-chair of the society and an independent energy analyst and author, said there are "significant economic possibilities" in producing combined heat and power (CHP) with nuclear reactors. He said: "With CHP, the reactor could produce roughly twice the value per installed capacity compared with just electricity production, while at the same time decarbonising heat production." He said nuclear is great for baseload needs, but with advanced technologies such as high temperature reactors and high temperature electrolysis, nuclear can also be used to decarbonise not just electricity, heat but also transportation fuels and many industries".

Date: 15 December 2017; Source: NucNet

Death from pollution dwarfs any other causes

Summary: Pollution kills at least nine million people and costs trillions of dollars every year, according to the most comprehensive global analysis to date, which warns the crisis “threatens the continuing survival of human societies”. “Pollution is one of the great existential challenges of the [human-dominated] Anthropocene era,” concluded the authors of the Commission on Pollution and Health, published in the Lancet on Friday. “Pollution endangers the stability of the Earth’s support systems and threatens the continuing survival of human societies. Pollution kills at least nine million people a year, and welfare losses from pollution amount are estimated at USD 4.6 trillion a year, equivalent to more than 6% of global GDP. The commission report combined data from the World Health Organisation (WHO) and elsewhere and found air pollution was the biggest killer, leading to heart disease, stroke, lung cancer and other illnesses. Outdoor air pollution, largely from vehicles and industry, caused 4.5 million deaths a year and indoor air pollution, from wood and dung stoves, caused 2.9 million. The next biggest killer was pollution of water, often with sewage, which is linked to 1.8 million deaths as a result of gastrointestinal diseases and parasitic infections. Workplace pollution, including exposure to toxins, carcinogens and second hand tobacco smoke, resulted in 800 000 deaths from diseases including pneumoconiosis in coal workers and bladder cancer in dye workers. Lead pollution, the one metal for which some data is available, was linked to 500 000 deaths a year.

Why it could be important? The editor-in-chief of the Lancet, Dr Richard Horton, and the executive editor, Dr Pamela Das, said: “No country is unaffected by pollution. Human activities, including industrialisation, urbanisation, and globalisation, are all drivers of pollution. We hope the commission findings will persuade leaders at the national, state, provincial and city levels to make pollution a priority. Current and future generations deserve a pollution-free world.”

Date: 20 October 2017; Source: <https://www.theguardian.com/environment/2017/oct/19/global-pollution-kills-millions-threatens-survival-human-societies>

The world is running out of sand

Summary: Pascal Peduzzi, a Swiss scientist and the director of one of the U.N.’s environmental groups, told the BBC last May that China’s swift development had consumed more sand in the previous four years than the United States used in the past century. In India, commercially useful sand is now so scarce that markets for it are dominated by “sand mafias”—criminal enterprises that sells material taken illegally from rivers and other sources, sometimes killing to safeguard their deposits. In the United States, the fastest-growing uses include the fortification of shorelines eroded by rising sea levels and more and more powerful ocean storms—efforts that, like many attempts to address environmental challenges, create environmental challenges of their own.

Why it could be important? In the industrial world, sand is “aggregate,” a category that includes gravel, crushed stone, and various recycled materials. Aggregate is the main constituent of concrete (eighty per cent) and asphalt (ninety-four per cent), and it’s also the primary base material that concrete and asphalt are placed on during the building of roads, buildings, parking lots, runways, and many other structures. A report published in 2004 by the American Geological Institute said that a typical American house requires more than a hundred tons of sand, gravel, and crushed stone for the foundation, basement, garage, and driveway, and more than two hundred tons if you include its share of the street that runs in front of it. A mile-long section of a single lane of an American interstate highway requires thirty-eight thousand tons. The most dramatic global increase in aggregate consumption is occurring in parts of the world where people who build roads are trying to keep pace with people who buy cars.

Date: 29 May 2017; Source: <http://www.newyorker.com/magazine/2017/05/29/the-world-is-running-out-of-sand>

GETTING IN TOUCH WITH THE EU

In person

All over the European Union there are hundreds of Europe Direct information centres. You can find the address of the centre nearest you at: https://europa.eu/european-union/contact_en

On the phone or by email

Europe Direct is a service that answers your questions about the European Union. You can contact this service:

- by freephone: 00 800 6 7 8 9 10 11 (certain operators may charge for these calls),
- at the following standard number: +32 22999696, or
- by electronic mail via: https://europa.eu/european-union/contact_en

FINDING INFORMATION ABOUT THE EU

Online

Information about the European Union in all the official languages of the EU is available on the Europa website at: https://europa.eu/european-union/index_en

EU publications

You can download or order free and priced EU publications from EU Bookshop at: <https://publications.europa.eu/en/publications>. Multiple copies of free publications may be obtained by contacting Europe Direct or your local information centre (see https://europa.eu/european-union/contact_en).

The European Commission's science and knowledge service

Joint Research Centre

JRC Mission

As the science and knowledge service of the European Commission, the Joint Research Centre's mission is to support EU policies with independent evidence throughout the whole policy cycle.



EU Science Hub

ec.europa.eu/jrc



@EU_ScienceHub



EU Science Hub - Joint Research Centre



Joint Research Centre



EU Science Hub



Publications Office
of the European Union

doi:10.2760/100724

ISBN 978-92-76-11442-0